Estandarización de gestión de TIC: un caso de ingeniería de estándares usando COBIT

Adrián Lara[a]

Escuela de Ciencias de la Computación e Informática
Universidad de Costa Rica
San José, Costa Rica

Marcelo Jenkins[b]

Escuela de Ciencias de la Computacion e Informática
Universidad de Costa Rica
San José, Costa Rica

Resumen

Este trabajo presenta un caso de ingeniería de estándares utilizando COBIT como punto de partida. Se genera una guía de implementación y evaluación para las Normas Técnicas de Gestión de TIC, que deben ser implementadas por todas las entidades que reciben fondos públicos en Costa Rica. La guía de evaluación es probada en una institución financiera gubernamental y se demuestra que la misma puede ser utilizada exitosamente para evaluar el nivel de cumplimiento de las Normas Técnicas de Gestión de TIC.

Palabras clave: Sistemas de información, Calidad de Proceso y Producto Software, Ingeniería de estándares, COBIT, SCAMPI

Abstract

This paper presents a case of standards engineering using COBIT as a starting point. We created an implementation and assessment guideline for an IT Management Standard that must be implemented by all entities that receive public funds in Costa Rica. The assessment guideline was tested in a government financial institution, thus demonstrating that it can be successfully used to assess the level of compliance with the IT Management Standard.

Keywords: Information systems, Process Quality and Software Product, Standard engineering, COBIT, SCAMPI

[a] Email: adrian.lara@ecci.ucr.ac.cr
[b] Email: marcelo.jenkins@ecci.ucr.ac.cr

1. Introducción

Las Tecnologías de Información y Comunicaciones (TIC) juegan un rol importante en la gestión de las organizaciones debido a que manejan grandes volúmenes de datos necesarios para la toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance. Es por esto que la administración de TIC debe considerarse dentro de toda organización como un componente estratégico, y es importante asegurarse que las TIC ayuden a cada organización a alcanzar sus metas, apoyando las actividades que se realizan [1].

Las organizaciones costarricenses que reciben financiamiento estatal, se encuentran sujetas a la fiscalización de la Contraloría General de la República (CGR). Esta entidad, consciente de la importancia de implementar buenas prácticas de gestión de TIC, publicó en julio de 2007 las Normas Técnicas de Gestión de TIC [1] (Normas de la CGR de aquí en adelante). Estas normas tienen como objetivo mejorar la gestión de TIC tomando los objetivos de control de COBIT como punto de partida [2]. Su implementación es obligatoria para todas aquellas entidades que se encuentren fiscalizadas por la CGR (más de 300 en este momento), por lo que tienen un alcance importante a nivel nacional.

Las Normas de la CGR procuran tomar de COBIT lo que resulte de mayor relevancia para el sector público costarricense. Con este objetivo, contienen cinco áreas y 25 requerimientos que tienen un alto grado de similitud con este marco de trabajo, como lo veremos más adelante. Sin embargo, la interpretación de los requerimientos de calidad descritos en estas Normas, tanto por parte de sus implementadores como por parte de sus evaluadores, ha resultado ser complicada y ambigua, según nuestra experiencia profesional. A continuación presentamos una descripción del problema que buscamos resolver en esta investigación.

1.1. Descripción del problema

A diferencia de otros estándares como COBIT [2] o CMMI [3], las Normas de la CGR no contienen un conjunto de prácticas sugeridas para guiar la implementación de los requerimientos. A modo de ejemplo, veamos el siguiente texto:

> *"La organización debe generar los productos y servicios de TIC de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo."* [1, pág. 2]

La cita corresponde al requerimiento 1.2 de las Normas de la CGR. No existe en dicho documento ninguna ayuda adicional para implementar lo solicitado. La labor de interpretación de lo que se pide en ese párrafo es compleja. Si comparamos con COBIT, vemos que el objetivo de control PO8 (ver [2] págs. 59-62) incluye una descripción similar al texto anterior, pero además menciona objetivos de control específicos que ayudan al implementador. Podemos observar que los objetivos de control específicos que propone COBIT permiten que la interpretación del requerimiento sea más sencilla y que el implementador disponga de información suficiente para poder cumplir con lo que le solicitan.

En CMMI, otro estándar internacionalmente reconocido, sucede algo similar, dado que las metas cuentan con prácticas e incluso sub prácticas. La Fig. 1 muestra cómo las Normas de la CGR tienen un vacío que nosotros proponemos llenar en esta investigación.

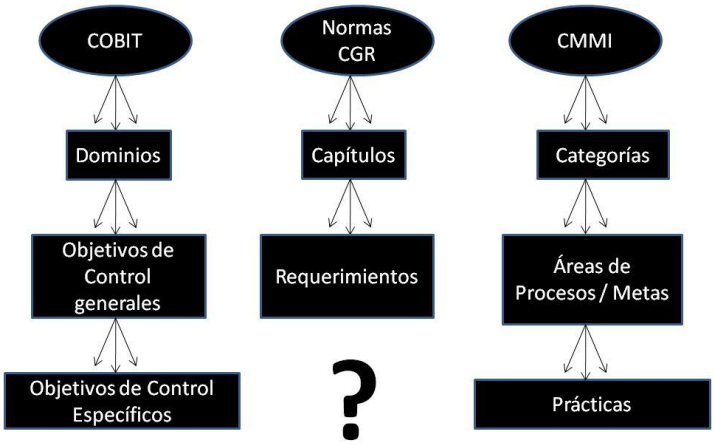


Fig. 1. Estructura de los estándares COBIT, CMMI y Normas de la CGR. Muestra la estructura de los estándares COBIT, CMMI y las normas de la CGR. A diferencia de COBIT y CMMI, las normas de la CGR no detallan la forma en que deben implementarse sus requerimientos.

Como podemos observar en la Fig. 1, no existen prácticas específicas que ayuden al implementador a determinar qué debe hacer para satisfacer un requerimiento. Asimismo, los evaluadores tampoco tienen claro qué deben solicitar como evidencia de cumplimiento de cada requerimiento.

1.2. Propuesta de solución

Nuestra propuesta de solución consiste en llenar ese vacío que evidencia la Fig. 1, proponiendo una guía de implementación y evaluación para las Normas de la CGR. Esto significa apoyarse en COBIT y completar, para cada requerimiento, cuáles son las prácticas que deberían implementarse para cumplir con lo que solicita el requerimiento. Además, proponemos un conjunto de evidencias que debe solicitar el evaluador para poder corroborar que cada requerimiento ha sido implementado adecuadamente.

En este punto surge una duda: Si las Normas de la CGR tienen bastantes puntos en común con COBIT, ¿por qué no usar este estándar como guía de implementación y evaluación? La respuesta es que las Normas de la CGR sólo tocan algunos de los temas de este estándar, no todos. Además, los requerimientos son similares pero no idénticos, por lo cual se requiere una guía de implementación especifica.

En este artículo describiremos los pasos metodológicos que seguimos para crear la guía mencionada. Luego, presentaremos los resultados obtenidos luego de probar dicha guía en una organización financiera costarricense. Finalmente, abordaremos aspectos importantes del trabajo futuro, que incluyen la medición del valor agregado percibido por los expertos con respecto a la guía propuesta. Antes, presentaremos los conceptos importantes relacionados con las Normas de la CGR.

2. Conceptos importantes

2.1. COBIT

COBIT es un conjunto de herramientas de gerencia de TIC publicado por el IT Governance Institute (ITGI) [4]. El ITGI es una organización sin fines de lucro, establecida en 1998 y se enfoca en ofrecer herramientas que ayuden a alinear las áreas de TIC a las empresas y sus objetivos. COBIT ayuda a cerrar la brecha que existe entre el negocio y las áreas de TIC, ofreciendo los controles mínimos que debería aplicar una organización de TIC [5]. Existen objetivos de control de alto nivel y otros de bajo nivel, separados en cuatro áreas (procesos):

- Planificar y Organizar (PO por sus siglas en inglés)
- Adquirir e Implementar (AI por sus siglas en inglés)
- Entregar y Dar soporte (DS por sus siglas en inglés)
- Monitorear y Evaluar (ME por sus siglas en inglés).

Los objetivos de control describen el estado al que se quisiera llegar una vez que se encuentre implementado el control. Existen 34 objetivos de control de alto nivel (PO1, PO2, AI1, DS1, ME1, etc.) y 318 específicos (PO1.1, PO1.2, PO AI1.1, etc.). Cada objetivo de control cuenta con una descripción que guía al implementador, indicándole cómo debe implementar cada control (a través de los objetivos de control específicos) y cuáles son las salidas esperadas [2].

La razón por la que COBIT es importante en este proyecto es porque las Normas de la CGR, que estudiaremos en la siguiente sección, toman lo más importante de él para estandarizar la gestión de TIC en el gobierno costarricense.

2.2. Normas de la CGR

La CGR elaboró y publicó las "Normas Técnicas para la Gestión y Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" con la intención de establecer una serie de requerimientos generales de carácter institucional y de acatamiento obligatorio, que pretenden hacer viable la administración desconcentrada de las tecnologías de información y comunicaciones y lograr una mayor agilidad y oportunidad en el desarrollo de los proyectos y procesos informáticos [1].

Estas normas se consideran básicas para establecer un marco de control y procuran una mejor gestión de las TIC, por lo que deben ser cumplidas como parte de la gestión institucional. El jerarca y los titulares subordinados, como responsables de esa gestión, deben establecer, mantener y evaluar procesos en sus departamentos de TIC para cumplir con estas normas [1], esto de conformidad con lo establecido en el Artículo 3 de la Ley de Control Interno No. 8292 del 31 de julio de 2002, que establece que "La Contraloría General de la República dictará la normativa técnica de control interno, necesaria para el funcionamiento efectivo del sistema de control interno de los entes y de los órganos sujetos a esta Ley. Dicha normativa será de acatamiento obligatorio y su incumplimiento será causal de responsabilidad administrativa". Es decir, esta ley obliga a los departamentos o direcciones de las TIC de las instituciones públicas a cumplir con las Normas Técnicas para la Gestión y Control de las Tecnologías de Información.

Las Normas contienen los siguientes cinco capítulos:

- Normas de aplicación general

- Planificación y organización
- Implementación de tecnologías de información
- Prestación de servicios y mantenimiento
- Seguimiento

Como podemos observar, los últimos cuatro son similares a los procesos definidos por COBIT. El primer capítulo, introducido por los diseñadores del estándar, incluye aspectos relacionados con la seguridad de la información, gestión de la calidad y otros temas [1].

La diferencia más importante entre las Normas de la CGR y COBIT radica en que las primeras únicamente incluyen requerimientos (que serían el equivalente a los objetivos de control de alto nivel de COBIT), pero no contienen objetivos de control específicos, que son precisamente los que indican cómo se debe implementar un requerimiento.

Sin embargo, es posible realizar un mapeo entre cada requerimiento de las Normas de la CGR y un objetivo de control de COBIT. Por ejemplo, existe una relación entre el requerimiento 1.2 de las Normas, llamado Gestión de la calidad y el objetivo de control PO8, que trata sobre Administrar la calidad. Este mapeo es parte de este proyecto de investigación y fue realizado por dos expertos en COBIT de la Escuela de Ciencias de Computación e Informática de la Universidad de Costa Rica. Este mapeo tiene un peso importante en este proyecto, ya que es el que permite pasar de los requerimientos de las Normas de la CGR a los objetivos de control de COBIT, para luego extraer los objetivos de control específicos más importantes.

A través del mapeo recién explicado y el detalle que ofrece COBIT, es posible crear la guía de implementación de las Normas de la CGR, como veremos más adelante. Como segunda parte, para poder comprender los pasos seguidos para crear la guía de evaluación, es necesario conocer los aspectos más importantes de la metodología SCAMPI.

2.3. SCAMPI

La metodología SCAMPI es utilizada para procesos de evaluación del modelo CMMI. Para conocer más detalles sobre dicho modelo, el lector puede referirse a [3].

SCAMPI propone una serie de reglas que buscan estandarizar la forma en que se realizan las evaluaciones. Es por esta razón que nuestra guía de evaluación se basa en esta metodología: para poder estandarizar la forma en que se evalúa el nivel de cumplimiento de las Normas de la CGR.

Para mayor detalle sobre los algoritmos de evaluación que propone SCAMPI, el lector puede referirse a [6]. En esta sección presentamos los aspectos más importantes que son necesarios para comprender la forma en que se creó la guía de evaluación.

Primero que todo, SCAMPI propone que el evaluador debe recolectar evidencias. Estas corresponden a artefactos (documentos, minutas, correos electrónicos) que demuestran de una u otra forma que una práctica ha sido implementada. Existen específicamente tres tipos de evidencia: directa, indirecta y pregunta de chequeo. El lector puede referirse a [6] para una explicación detallada de dichos términos.

También es importante mencionar que SCAMPI sugiere que, con base en el

análisis de las evidencias, se determine el nivel de cumplimiento de una práctica, la cual puede estar completamente implementada, ampliamente implementada, parcialmente implementada o no implementada. El detalle de este algoritmo se puede encontrar en [7].

Luego, el nivel de implementación de todas las prácticas que deben ser implementadas para cumplir con un requerimiento, indica el nivel de satisfacción del mismo. Por ejemplo, SCAMPI exige que todas las prácticas deban estar ampliamente o completamente implementadas para que una meta (o requerimiento) pueda ser considerada satisfecha. Nuevamente, el detalle de estos algoritmos puede ser consultado en [7].

Finalmente, SCAMPI exige que se clasifiquen las prácticas en dos categorías: organizacional o por proyecto. Por ejemplo, la creación de un plan estratégico de TIC debería hacerse una única vez por cada organización, por lo que representa una práctica organizacional. Sin embargo, ejecutar un conjunto de pruebas de aceptación correspondería a una práctica que debe revisarse para varios proyectos y no únicamente una vez a nivel organizacional. Sobre este tema, SCAMPI indica que las prácticas organizacionales deben ser evaluadas únicamente una vez y las que corresponden a proyectos deben solicitarse para cuatro proyectos de la organización evaluada [7].

Como veremos más adelante, nuestra guía de evaluación toma en cuenta lo explicado anteriormente con respecto a SCAMPI.

3. Metodología

Esta sección explica la metodología seguida para crear una guía de implementación de las normas de la CGR, primero, y cómo especificar una guía de evaluación, después. La Fig. 2 resume todos los pasos metodológicos que explicaremos detalladamente a continuación.

Fig. 2. Resumen de pasos metodológicos. Se muestran los pasos metodológicos que se realizaron durante esta investigación.

3.1. Crear la guía de implementación

El objetivo de la guía de implementación es darle a quienes deban implementar las Normas de la CGR una serie de pasos a seguir para poder cumplir con lo solicitado en cada requerimiento. Para generarla, se siguieron los pasos mostrados en la Fig. 3.

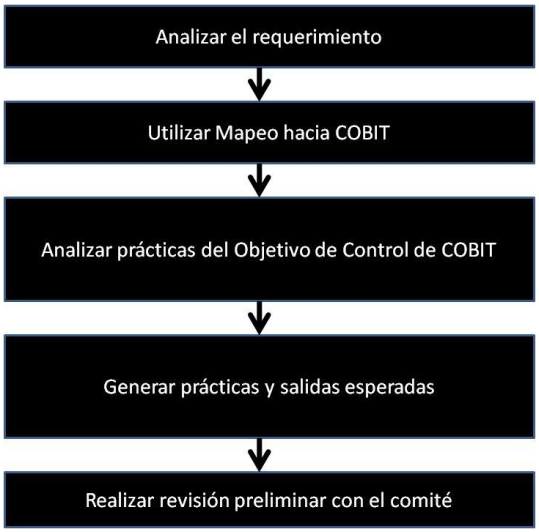


Fig. 3. Pasos metodológicos para crear la guía de implementación. Se muestran los pasos metodológicos que se realizaron para crear la guía de implementación.

El proceso de generación de la guía consistió en ejecutar los pasos descritos en la Fig. 3 para cada uno de los requerimientos de las Normas de la CGR. A partir de un análisis de los requerimientos y utilizando el mapeo que mencionamos en la sección 2, determinamos con base en los objetivos de control específicos de COBIT, cuáles eran las prácticas que debían implementarse para cumplir con cada requerimiento. De esta forma generamos, para cada requerimiento de las normas, una serie de prácticas que deben ser implementadas.

Debido a la dificultad que conlleva determinar la completitud o la calidad de una guía de implementación, la misma fue validada a través de un comité experto, el cual aportó comentarios y sugerencias a la lista de prácticas propuestas.

Una vez concluida la guía de implementación, el segundo problema que busca resolver esta investigación es ¿cómo se debe evaluar el nivel de cumplimiento de las Normas de la CGR? En la siguiente sección explicaremos los pasos seguidos para crear la guía de evaluación.

3.2. Crear la guía de evaluación

La guía de evaluación de las Normas de la CGR da todas las indicaciones necesarias para que un evaluador pueda seguirlas y ser capaz de determinar cuál es el nivel de cumplimiento a la hora de evaluar a una organización de TIC. La Fig. 4 muestra el detalle de pasos seguidos para crear esta guía.

Para crear la guía de evaluación nos basamos en la metodología SCAMPI,

descrita previamente en la sección de conceptos importantes. El primer paso para crear una guía que siga los pasos de SCAMPI consistió en clasificar cada práctica propuesta en la guía de evaluación como organizacional o por proyecto. Luego se definieron las evidencias (directas, indirectas y preguntas de chequeo) que deben ser requeridas por el evaluador para determinar el nivel de cumplimiento de un requerimiento.

Para determinar el nivel de implementación de una práctica, con base en las evidencias analizadas, así como para establecer el nivel de satisfacción de un requerimiento con base en las prácticas evaluadas, se utilizaron las mismas reglas establecidas por SCAMPI que describimos en la sección 2.3.

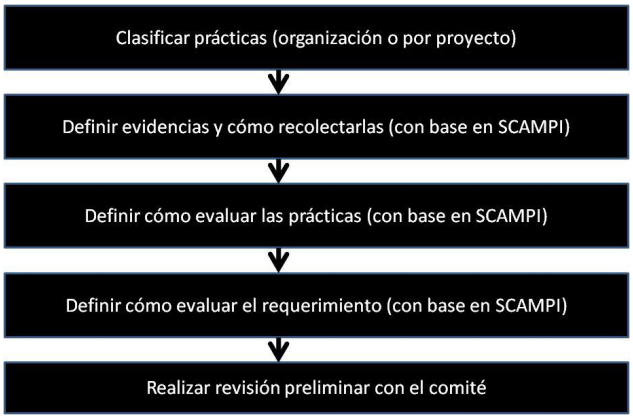


Fig. 4. Pasos metodológicos para crear la guía de evaluación. Se muestran los pasos metodológicos seguidos para generar la guía de evaluación.

Como resultado de la guía de evaluación, quien se encuentre evaluando el nivel de cumplimiento de las Normas de la CGR en una organización ya no debe interpretar el requerimiento ni decidir qué va a evaluar; únicamente debe recolectar las evidencias establecidas por la guía. Una vez analizadas las evidencias, el resto del algoritmo de evaluación es estándar y tomado de SCAMPI. Esto mejora la estandarización de las evaluaciones, dado que la única subjetividad se da a la hora de determinar la validez de una evidencia, así como al momento de identificar debilidades.

Al igual que con la guía de implementación, la de evaluación también fue validada con expertos, quienes externaron sus opiniones con respecto a las evidencias directas, indirectas y preguntas de chequeo propuestas por la guía. Posteriormente, dieron su visto bueno al documento final.

Antes de continuar con los pasos metodológicos, consideramos conveniente ilustrar con un ejemplo el resultado final de haber creado una guía de implementación y evaluación para cada uno de los requerimientos de las Normas.

En la descripción del problema analizamos el siguiente texto:

> *"La organización debe generar los productos y servicios de TIC de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo."* [1, pág. 2]

Como resultado de esta investigación, nuestra guía de implementación indica

que, para cumplir con lo establecido, se deben implementar cuatro prácticas: prácticas de calidad, enfoque en el cliente, mejora continua y auditoría. Cada práctica se encuentra acompañada de una explicación detallada de lo que se espera por parte del auditor.

Asimismo, la guía de evaluación establece que las cuatro prácticas mencionadas fueron clasificadas como organizacionales e indican al evaluador que debe solicitar evidencias directas e indirectas, entre las cuales se incluyen los estándares y prácticas de calidad implementados, las políticas de atención al cliente, las políticas de mejora continua, los procesos y procedimientos de auditoría definidos, así como los informes generados durante estas revisiones.

Este nivel de detalle es alcanzado para cada uno de los requerimientos de las Normas. Así garantizamos que los implementadores y evaluadores tienen una guía para cada uno de ellos.

En este punto es importante notar lo siguiente: al ser 25 requerimientos y cada uno contar en promedio con 4 prácticas específicas, y al contar cada práctica con aproximadamente tres evidencias, podemos observar que la lista de artefactos que deben ser revisados por el evaluador es sumamente grande, máxime si algunas prácticas deben ser evaluadas cuatro veces. Esto da pie al uso de una herramienta de software que simplifique la recolección de evidencias así como la visualización de los resultados.

3.3. Uso de la herramienta Appraisal Assistant

Appraisal Assistant es una herramienta de software libre desarrollada por el *Software Quality Institute* de la *Griffith University* [8], diseñada para apoyar procesos de evaluación que necesiten recolectar, visualizar y analizar evidencias. Su objetivo es simplificar el manejo de dichas evidencias y dentro de las metodologías de evaluación que soporta se encuentra SCAMPI. Se puede encontrar documentación al respecto en [8]. Es importante mencionar que, si bien la versión más actualizada de SCAMPI es 1.3, la herramienta soporta hasta 1.2. Por esta razón nuestra guía se basa en esta última.

Esta herramienta permite la incorporación de nuevos modelos, por lo que es posible prepararla para apoyar evaluaciones de las Normas de la CGR. En efecto, una consecuencia de la creación de las guías de implementación y evaluación es que le dimos a las Normas de la CGR una estructura jerárquica, con áreas, requerimientos, prácticas y evidencias, al igual que otros estándares como CMMI. Por esta razón es posible utilizar esta herramienta en las evaluaciones y las ventajas de recolección y visualización podrán ser apreciadas en la sección de resultados. Antes de eso, explicamos a continuación los pasos seguidos para realizar una evaluación del nivel de cumplimiento de las Normas de la CGR en una entidad financiera de Costa Rica, utilizando la guía de evaluación así como la herramienta Appraisal Assistant.

3.4. Evaluación del nivel de cumplimiento de las Normas de la CGR en una organización de TIC

El objetivo de realizar una evaluación del nivel de cumplimiento de las Normas de la CGR en una organización de TIC es demostrar la aplicabilidad de la guía de evaluación. La misma también fue validada por expertos, pero esta experiencia

permite demostrar su aplicabilidad real.

Para evaluar el nivel de cumplimiento de las normas de la CGR en esta entidad, seguimos la metodología de auditoría propuesta por Muñoz Razo en [9]. Este autor propone tres etapas: planificación de la auditoría, ejecución de la misma y dictamen de los resultados, tal y como se muestra en la Fig. 5.

Fig. 5. Pasos metodológicos para realizar la evaluación en una organización de TIC. Se muestran las etapas llevadas a cabo para realizar la evaluación del nivel de cumplimiento de las Normas de la CGR en la entidad financiera.

Para una revisión detallada del contenido de cada paso metodológico, se recomienda revisar [9]. En la siguiente sección analizaremos los resultados obtenidos, primeramente, durante la evaluación del nivel de cumplimiento de las Normas de la CGR en esta entidad. Posteriormente, analizaremos lo que hemos logrado al proponer estas guías de implementación y evaluación.

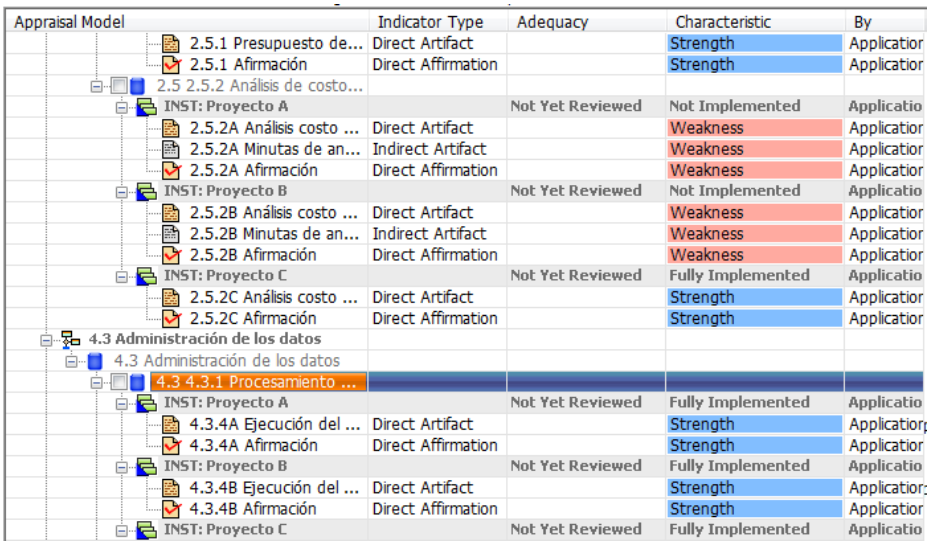
4. Resultados

Sin duda alguna el producto más importante de esta investigación es la guía de implementación y evaluación propuesta. En la sección 3.2 vimos un ejemplo de los resultados obtenidos para uno de los requerimientos, a modo de ilustración de la metodología. La aplicabilidad de esta guía se probó utilizándola para evaluar el nivel de cumplimiento de las Normas en una organización. A continuación mostramos los resultados obtenidos.

4.1. Resultados de la evaluación ejecutada en la entidad financiera

De los 25 requerimientos que incluyen las Normas de la CGR, presentaremos la evaluación del nivel de cumplimiento para cinco de ellos. Esta muestra permite visualizar los posibles resultados que se pueden obtener al utilizar la guía de evaluación.

La Fig. 6 muestra la interfaz de Appraisal Assistant utilizada para recolectar todas las evidencias que fueron necesarias, siguiendo la guía de evaluación.



Appraisal Model	Indicator Type	Adequacy	Characteristic	By
2.5.1 Presupuesto de...	Direct Artifact		Strength	Applicatior
2.5.1 Afirmación	Direct Affirmation		Strength	Applicatior
2.5 2.5.2 Análisis de costo...				
INST: Proyecto A		Not Yet Reviewed	Not Implemented	Applicatio
2.5.2A Análisis costo ...	Direct Artifact		Weakness	Applicatior
2.5.2A Minutas de an...	Indirect Artifact		Weakness	Applicatior
2.5.2A Afirmación	Direct Affirmation		Weakness	Applicatior
INST: Proyecto B		Not Yet Reviewed	Not Implemented	Applicatio
2.5.2B Análisis costo ...	Direct Artifact		Weakness	Applicatior
2.5.2B Minutas de an...	Indirect Artifact		Weakness	Applicatior
2.5.2B Afirmación	Direct Affirmation		Weakness	Applicatior
INST: Proyecto C		Not Yet Reviewed	Fully Implemented	Applicatio
2.5.2C Análisis costo ...	Direct Artifact		Strength	Applicatior
2.5.2C Afirmación	Direct Affirmation		Strength	Applicatior
4.3 Administración de los datos				
4.3 Administración de los datos				
4.3 4.3.1 Procesamiento ...				
INST: Proyecto A		Not Yet Reviewed	Fully Implemented	Applicatio
4.3.4A Ejecución del ...	Direct Artifact		Strength	Applicatior
4.3.4A Afirmación	Direct Affirmation		Strength	Applicatior
INST: Proyecto B		Not Yet Reviewed	Fully Implemented	Applicatio
4.3.4B Ejecución del ...	Direct Artifact		Strength	Applicatior
4.3.4B Afirmación	Direct Affirmation		Strength	Applicatior
INST: Proyecto C		Not Yet Reviewed	Fully Implemented	Applicatio

Fig. 6. Interfaz de recolección de evidencias de Appraisal Assistant. Se muestra un segmento de las evaluaciones levantadas durante la evaluación, usando la interfaz gráfica de Appraisal Assistant.

Podemos observar cómo gráficamente se indica si se trata de una evidencia directa, indirecta o una pregunta de chequeo. Asimismo, es posible indicar si se trata de una fortaleza y una debilidad. El resultado es positivo porque se puede diferenciar rápidamente cuáles evidencias corresponden a cada práctica, así como el tipo de evidencia.

Posteriormente, con base en el análisis de las evidencias, es posible determinar gráficamente el nivel de cumplimiento de cada práctica, así como se muestra en la Fig. 7.

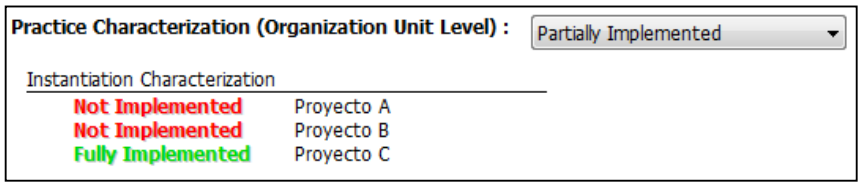


Fig. 7. Interfaz de evaluación del nivel de cumplimiento de una práctica. Se muestra un ejemplo de evaluación del nivel de cumplimiento de una práctica clasificada como por proyecto. Se observa que hay dos proyectos que no implementan adecuadamente la práctica y hay uno que si lo hace. Luego de la agregación de estos tres resultados, la práctica queda evaluada como parcialmente implementada.

Finalmente, la herramienta permite visualizar el nivel de cumplimiento de cada práctica, como se muestra en la Fig. 8.

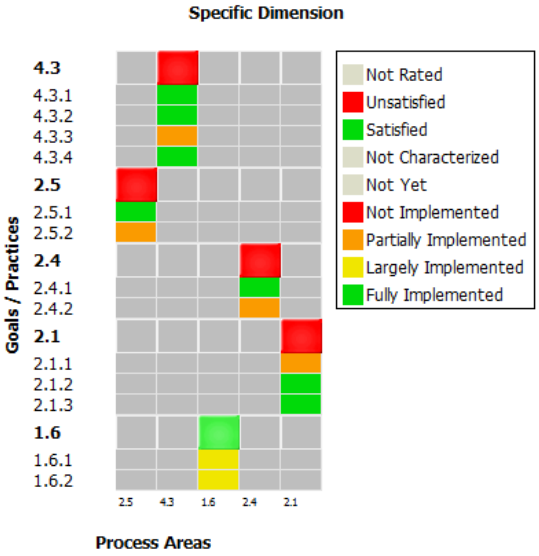


Fig. 8. Interfaz de visualización de resultados de Appraisal Assistant. Se muestra el resultado final de la evaluación de los cinco requerimientos.

En la siguiente sección analizaremos los resultados mostrados en la Fig. 8.

4.1.1 Análisis de los resultados mostrados

Podemos observar que existen requerimientos cuyo nivel de cumplimiento es satisfactorio (1.6). Asimismo, hay otros requerimientos donde existen una o más prácticas que no se encuentran completamente o ampliamente implementadas, por lo que el nivel de cumplimiento del requerimiento se ve afectado (2.1, 2.4, 2.5 y 4.3).

Esta evaluación permitió a la entidad financiera identificar claramente cuáles son las prácticas que no se están implementando en la forma esperada. En el caso del requerimiento 2.1, se observa que no existe un plan estratégico, debido a que lo que se utiliza actualmente se acerca más a un plan operativo anual y no se documenta una estrategia con metas a mediano y largo plazo.

La entidad tampoco cuenta con un plan de capacitación específico para cada área de TIC, por lo que no se considera satisfecho el requerimiento 2.4. En el caso del requerimiento 2.5, podemos observar que se trata de una práctica clasificada como "por proyecto", por lo que se evalúan cuatro proyectos y dos de ellos no muestran resultados satisfactorios. Por esta razón, el requerimiento 2.5 tampoco se encuentra satisfecho.

Finalmente, el caso del requerimiento 4.3 es interesante de analizar ya que no existe un procedimiento de desecho de datos, aunque algunas áreas cuentan con

guías que documentan cómo hacerlo. Por esta razón, el hecho de que exista una evidencia indirecta y una afirmación hacen que la práctica se encuentre parcialmente implementada, pero esto no es suficiente para declarar el requerimiento como satisfecho.

Las ventajas de haber generado una estructura jerárquica para las Normas de la CGR y de haber usado la herramienta Appraisal Assistant saltan a la vista a la hora de visualizar y analizar los resultados de esta evaluación. En la siguiente sección estudiaremos detalladamente cuáles son las ventajas que hemos encontrado como producto de esta investigación.

4.2. Análisis de los resultados de la investigación

4.2.1 Estandarización de la implementación y evaluación de las Normas de la CGR

Como lo mencionamos anteriormente, hemos visto en nuestra experiencia profesional las dificultades que han existido para decidir cómo se deben implementar las Normas de la CGR y cómo deben ser evaluadas. Los requerimientos de las Normas de la CGR fueron diseñados intencionalmente en forma abierta, con la intención de que organizaciones de tamaños muy disímiles pudieran interpretarlos libremente para implementarlos. En efecto, dichos requerimientos aplican a entidades con presupuestos de TIC sumamente alto (entidades bancarias, por ejemplo), pero también a organizaciones con áreas de TIC pequeñas.

Sin embargo, la consecuencia de esa decisión fue la gran dificultad de interpretación de los requerimientos que existe tanto en los implementadores como en los evaluadores. Por esta razón, proponer una forma estándar para evaluar y para implementar constituye un gran apoyo al sector de gobierno, dado que permite ahorrar un esfuerzo de interpretación que, en este momento, debe ser efectuado en forma independiente por cualquier entidad que deba implementar o evaluar las Normas de la CGR.

Aquí también es importante recalcar la importancia de haber utilizado la metodología de evaluación SCAMPI, la que busca que, en condiciones similares, dos evaluaciones generen el mismo resultado final [7]. Esto mismo es lo que hemos buscado en esta propuesta, dado que buscamos estandarizar la forma en que se evalúan dichas Normas. El hecho de que se utilice siempre el mismo algoritmo aumenta en gran medida la objetividad de las evaluaciones realizadas.

4.2.2 Creación de una estructura jerárquica para las Normas de la CGR

Otro aporte importante de las guías de implementación y evaluación de las Normas de la CGR es haber propuesto una estructura jerárquica para este modelo. En efecto, es difícil determinar cómo evaluar un conjunto de texto que no se encuentra estructurado. Por esa misma razón, otros modelos como CMMI han propuesto una estructura jerárquica, donde para determinar el nivel de cumplimiento de un requerimiento es necesario evaluar primero cada práctica, para lo que hay que haber analizado cada evidencia. Así, analizando únicamente evidencias finales, es posible determinar el nivel de cumplimiento de un requerimiento. De igual forma, es posible rastrear un incumplimiento de un requerimiento hasta un documento final, lo cual permite detectar con mayor facilidad qué debe mejorarse para poder

cumplir con un requerimiento.

El hecho de haber generado esta estructura jerárquica similar a la de CMMI permite también que herramientas diseñadas para evaluaciones SCAMPI puedan ser utilizadas para simplificar los procesos de evaluación de las Normas de la CGR. Esto nos lleva a otro aporte de nuestra investigación: el uso de la herramienta Appraisal Assistant.

4.2.3 Ventajas del uso de la herramienta Appraisal Assistant

Las ventajas del uso de la herramienta Appraisal Assistant quedaron en evidencia a la hora de visualizar los resultados de la evaluación realizada en la entidad financiera. Primero, se simplifica la recolección de las evidencias ya que permite gráficamente identificar si se trata de una evidencia directa, indirecta o pregunta de chequeo, así como si representa una fortaleza o una debilidad. Adicionalmente, se puede acceder directamente al documento utilizado como evidencia mediante hipervínculos. En nuestra experiencia, este proceso de recolección es considerablemente más sencillo que utilizando otras herramientas.

La segunda ventaja de la herramienta se presenta a la hora de aplicar los algoritmos propuestos por SCAMPI. Por ejemplo, a la hora de determinar el nivel de cumplimiento de una práctica con base en las evidencias, a la hora de agregar distintas evidencias para evaluar una misma práctica o también a la hora de determinar el nivel de satisfacción de un requerimiento. Todos estos pasos, que en otras herramientas deben ejecutarse en forma manual, son realizados automáticamente por Appraisal Assistant, lo cual representa un ahorro importante en el tiempo de ejecución de las evaluaciones. En esta misma línea, la herramienta es capaz de indicar si la recolección de evidencias cumple con la metodología SCAMPI. Por ejemplo, si para una práctica ya se recolectó una evidencia directa y una pregunta de chequeo, entonces la interfaz indica que ya se está cumpliendo con SCAMPI. Al contrario, si la recolección de evidencia no cumple con la metodología, entonces así lo indica Appraisal Assistant.

Finalmente, la visualización de los resultados también es más agradable utilizando Appraisal Assistant. Como pudimos ver en los resultados de la evaluación realizada, es sumamente sencillo identificar cuáles son las evidencias que generan incumplimientos. También se simplifica la visualización de los resultados finales, ya que el uso de colores ayuda a identificar rápidamente cuáles requerimientos se encuentran satisfechos y cuáles no.

5. Trabajo futuro

Este proyecto de investigación incluye un paso que aún no ha sido concluido. El mismo tiene como meta medir el valor percibido por los usuarios de la organización financiera evaluada y por los expertos de la Contraloría General de la República de las guías de implementación y evaluación propuestas.

El objetivo de esto es conseguir la opinión especializada de quienes diseñaron las Normas de la CGR, así como la de los funcionarios encargados de implementar dichas Normas. Esto implica realizar una investigación cualitativa que permita contestar la siguiente interrogante: ¿Cuál es el aporte, en cuanto a utilidad, de la guía de evaluación propuesta? Desarrollamos un instrumento que nos permitirá conocer la opinión de los expertos de la organización de TIC evaluada y de la CGR con respecto a eso. En caso de que se detecte que sí existe una diferencia significativa, este instrumento nos permitirá también identificar cuáles son los

aspectos más importantes que, según los expertos, hacen significativa dicha diferencia.

6. Conclusiones

En este artículo describimos el problema que se presenta a la hora de interpretar los requerimientos de las Normas de la CGR y propusimos como solución generar una guía de implementación y una de evaluación para dicho modelo. La primera contiene las prácticas que deben ser implementadas para cumplir con lo solicitado por cada requerimiento. La segunda incluye la clasificación de los requerimientos, así como las evidencias directas, indirectas y preguntas de chequeo que deben ser solicitadas por quien evalúe el nivel de cumplimiento de las Normas.

Demostramos que es posible generar dicha guía y que la misma es usable, dado que logramos utilizarla para evaluar el nivel de cumplimiento de las Normas de la CGR. Esto genera que tanto los implementadores como los evaluadores cuenten con una guía que pueden utilizar para tales efectos.

Dentro de las ventajas de estas guías encontramos que estandarizan la forma en que se implementan y se evalúan los requerimientos de las Normas y se genera una estructura jerárquica para las mismas, formando prácticas y evidencias. Esto permitió que fuera posible utilizar una herramienta de software preparada para realizar evaluaciones en modelos jerárquicos como CMMI, por lo que fue posible aprovechar las ventajas de recolección y visualización que ofrece Appraisal Assistant.

El siguiente paso de esta investigación consiste en medir el valor percibido por los expertos de la CGR encargados de la creación de las Normas, así como de los funcionarios de la entidad financiera evaluada encargados de implementar las Normas en esa institución.

Referencias bibliográficas

[1] Contraloría General de la República. “Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)”. Aprobadas mediante Resolución del Despacho de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007. Publicado en La Gaceta Nro.119 del 21 de junio, 2007.

[2] IT Governance Institute. “COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models”. 2007.

[3] Software Engineering Institute, Carnegie Mellon. CMMI, Capability Maturity Model Integration (CMMI). URL: http://www.sei.cmu.edu/cmmi/index.cfm

[4] ISACA: Frameworks and related products that help professionals attain value from information systems. http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/CobiT_Products.pdf

[5] IT Governance Institute: About ITGI. http://www.itgi.org/template_ITGI.cfm?Section=About_ITGI&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=41668

[6] Ahern, Dennis; Armstrong, Jim; Clouse, Aaron; Ferguson, Jack; Hayes, Will; Nidiffer, Kenneth. “CMMI SCAMPI Distilled. Appraisals for Process Improvement”. Editorial Addison-Wesley. 2005.

[7] Software Engineering Institute, Carnegie Mellon. Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Version 1.2: Class A Team Training.

[8] Software Quality Institute, Griffith University. An Overview of Appraisal Assistant, A tool to support process assessment / appraisal. URL: www.sqi.gu.edu.au/AppraisalAssistant/AppraisalAssistantDemo.ppt

[9] Muñoz Razo, C., Auditoría en sistemas computacionales. Pearson Educación, 2002.