Usando Cobit para cumplir la normativa de TI emitida por la CGR

Resumen

El principal dilema que deben resolver las instituciones cuando una entidad supervisora emite una normativa de acatamiento obligatorio está en identificar las referencias técnicas que deben utilizarse para construir los instrumentos que permitan dar cumplimiento a la normativa.

La Contraloría General de la República de Costa Rica (CGR) emitió una normativa en la temática de las tecnologías de información cuyo propósito es orientar el fortalecimiento de la gestión de TI.

En este artículo podrá identificar porqué COBIT contiene un conjunto fundamental de ayudas para que la empresa pueda orientar mejor los esfuerzos que debe ejecutar para alcanzar un cumplimiento cabal de lo dispuesto por el ente contralor.

Autor: Manuel Arauz Montero, consultor de

T I AUDISEG en temas de gobierno de TI y seguridad de la información.

COBIT un estándar en gobierno de TI

COBIT cuyas siglas tienen el siguiente significado en idioma inglés (Control Objective for Information Technology) es hoy reconocido mundialmente como un marco de referencia para la implementación de un mejor gobierno o gestión de TI.

Esto quiere decir que todo el instrumental que se ha desarrollado por la ITGI dentro de lo que conocemos como COBIT pretende que las organizaciones alcancen un alineamiento adecuado entre los objetivos institucionales y los objetivos trazados en materia de tecnologías de información, que logren un adecuado retorno de la inversión que realicen en TI, que posean una correcta administración de los riesgos en esta materia y dispongan de un apropiado marco de control interno.

Como puede verse, un proceso de gobierno de TI es un esfuerzo en el cual participa toda la organización y para el cual se requiere contar con un adecuado conjunto de instrumentos.

COBIT mediante la identificación de procesos y objetivos de control, con la conceptualización de los niveles de madurez por proceso, de indicadores de gestión y rendimiento, con la propuesta de matrices RACI y con otro instrumental que provee es la herramienta más adecuada en la que las empresas pueden apoyarse para un proceso de gobierno de TI. No es la única, guías o referencias como ITIL, PRINCE2, CMMI o ISO 27001 son igualmente instrumentos valiosos que pueden servir de apoyo, pero estos últimos no enfocan integralmente la gestión de TI sino componentes importantes de ella, por eso COBIT se conoce como el estándar actual en gobierno de TI.

¿Por qué COBIT para cumplir con la normativa de TI?

Esta es una pregunta básica que conviene plantearse.

La primera argumentación que podemos ofrecer para ello está en el propósito de la normativa misma. De su lectura es fácil deducir que lo que la CGR preparó es una normativa que impulsa la gobernabilidad de TI en las entidades públicas costarricenses.

Pues bien, si el propósito es el gobierno de TI y la normativa contiene 26 directrices específicas divididas en 5 apartados que definen elementos importantes que una entidad pública debe cumplir

en materia de la gestión de TI, pues es necesario identificar un instrumento de gobierno de TI que sirva para enfocar los esfuerzos hacia la dirección correcta.

Ese ejercicio rápidamente permite homologar los alcances planteados en las diferentes directrices con los procesos que contiene Cobit y al hacer ese emparejamiento ya se logran grandes avances ya que a partir de ahí se puede utilizar el marco de referencia de COBIT para desarrollar las siguientes etapas de un proceso de cumplimiento de una normativa.

Cuáles son esas etapas? Primero identificar el estado actual de cumplimiento de la normativa que se tiene, segundo determinar cuál es la brecha con respecto a lo que estipula la normativa y trazar un plan de acciones para cerrar la brecha existente, tercero ejecutar ese plan de acciones y finalmente volver a evaluar el estado alcanzado para valorar si conviene ejecutar un nuevo proceso de ajustes dentro de un enfoque de mejoramiento continuo.

¿Puede ayudarme COBIT en esas etapas?

Indudablemente que si, logrando un paralelismo entre la normativa y los procesos de COBIT es posible utilizar los niveles de madurez de COBIT para determinar el nivel actual de la organización y determinar si dicho nivel de madurez sirve para dar cumplimiento a la normativa.

Si no fuese suficiente, podemos nuevamente utilizar los niveles de madurez para definir cuál es la brecha existente, es decir, cuál es el nivel de madurez que debieramos alcanzar. Acá es importante tener presente que la normativa de la CGR fija un plazo hasta julio 2009 para que se dé un cumplimiento de la normativa, por lo que la entidad deberá valorar hasta donde podrá llegar con los recursos disponibles en el plazo definido por la CGR y tener presente que si no se llegara a alcanzar un cumplimiento total de lo dispuesto en la normativa se deberá visualizar un proceso de mejoramiento continuo que permita en un plazo un poco mayor ir logrando el cumplimiento deseado.

Pues bien, fijado el nivel de madurez por alcanzar, nuevamente COBIT con su instrumental nos permite identificar productos a desarrollar y actores y con esos insumos elaborar un plan de trabajo con prioridades bien definidas ya que un proceso de implementación de gobierno de TI requiere de una correcta definición de la secuencia de ejecución de las acciones para favorecer la maduración de los instrumentos.

Ejecutadas las acciones igualmente mediante indicadores de COBIT podemos valorar la gestión de TI y confirmar que efectivamente hemos alcanzado un nivel de madurez mayor y disponemos de medios que propician un mejor gobierno de TI.

Esto es igualmente aplicable para los casos de las entidades financieras y bursátiles que deban cumplir con la normativa de la SUGEF o la SUGEVAL, donde de la misma manera, el instrumental de COBIT ayuda a que los esfuerzos de mejora del gobierno de TI se hagan de forma planificada, eficaz y eficiente.

Nuestra experiencias como consultores en procesos de esta naturaleza nos ha confirmado que si se utiliza de forma correcta el COBIT y en los casos requeridos se complementa este estándar con otras guías como el ITIL, PRINCE2, ISO 27001, las organizaciones pueden lograr grandes beneficios en materia de gobierno de TI.

Cumplir una normativa es un objetivo regulatorio, mejorar en gobierno de TI es un imperativo organizacional que se traduce en beneficios directos para la empresa.

Aprovechemos la oportunidad que ofrece la promulgación de esta normativa para convencer a nuestra organización de los beneficios de los procesos de gobierno de TI correctamente conceptualizados y en los cuales se utilizan los instrumentos correctos.