Nueva regulación para la gestión de Tecnología de la Información (TI) para el sector financiero costarricense. Por David R. Rodríguez Calderón. Profesional en Auditoría, Control y Gestión de Recursos Tecnológicos y Administración de Proyectos.

Nota Aclaratoria:

Este es un artículo Técnico con fines didácticos. Los comentarios no expresan una posición u opinión de las empresas o instituciones con la que estoy relacionado, el fin del artículo es realizar un acercamiento al medio sobre los elementos más relevantes del reglamento de gestión de TI, en caso de ser publicado requiere mi autorización expresa y es a título personal como Profesional en Auditoría, Control y Gestión de Recursos Tecnológicos y Administración de Proyectos.

Retrospectiva

El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), trabajó durante los últimos tres años, en definir una regulación consolidada para la gestión de TI. Esta normativa se fundamenta en la experiencia adquirida con la norma SUGEF 14-09, así como en un conjunto de estándares, mejores prácticas, lecciones aprendidas y los fraudes causados en la gestión operativa de negocios complejos con un diverso ecosistema tecnológico heredado. Dicha normativa fue publicada en el Alcance a la Gaceta No 80, del 17 de abril del 2017 y entra a regir a partir del mes de mayo del presente año.

El reto de las entidades del sector

Las entidades tiene el reto de garantizar la seguridad, auditabilidad y disponibilidad de la información y de los servicios ofrecidos a sus clientes, mediante la definición e implementación de un marco de gestión de TI basado en procesos, el cual debe ser planificado, implementado y documentado de forma progresiva. Dicho marco tiene que sustentar las estructuras, procesos o líneas de negocio y las actividades significativas de la entidad considerando el principio de proporcionalidad. (Naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad, riesgos y dependencia tecnológica).

En la actualidad, las entidades deben procurar visualizar TI como un proceso de apoyo y como un proveedor de servicios, por este motivo, el reglamento incorpora el concepto de la Unidad de TI para facilitar su modelo de gestión (Individual o Corporativa para aquellos grupos o conglomerados financieros registrados en el territorio nacional). Conforme a lo anterior, los procesos y servicios de TI pueden estar externalizados según los requerimientos o necesidades del negocio, sin embargo el reglamento enfatiza que la responsabilidad del gobierno, gestión y seguridad de información de aquellos elementos tercerizados, recae en las entidades supervisadas y sus órganos de gobierno y control.

Por ultimo, las entidades deben propiciar una gobernabilidad corporativa por lo que introduce el concepto de Gobierno de TI como una estructura con actividades y propósitos orientados a la generación de valor, a través de la obtención de los beneficios, la optimizacion de los recursos y un nivel de riesgo aceptable, siempre considerando las necesidades de los interesados y delimitando claramente las responsabilidades y actividades propias de gobierno y gestion.

Modelo de Supervisión

Enmarcado dentro del Modelo de Supervisión Basada en Riesgos (SBR), este reglamento se caracteriza por migrar de un modelo basado en reglas hacia un enfoque donde la entidad es responsable de gestionar de forma integral los riesgos del negocio con el fin de identificar y establecer las medidas de mitigación de los riesgos asociados con TI.

Uno de los principios del modelo de SBR es conocer al supervisado, por esta razón el reglamento solicita que cada entidad elabore y mantenga actualizado de forma anual su perfil tecnológico el cual comprende una descripción de la estructura organizacional, los procesos y la infraestructura de TI de dicha entidad.

Siguiendo con la línea del modelo de SBR, se puede observar en el reglamento la función de la Auditoría de TI, la cual se visualiza como un servicio externalizado en el que las superintendencias se apoyan para realizar la revisión y aplicación del marco de gestión de TI. Adicionalmente el reglamento define los elementos mínimos para el proceso de auditoría introduciendo en el reglamento de Auditores Externos los elementos de control prudenciales requeridos por el supervisor.

Alcance de la Norma

Las entidades incluidas en el alcance de la norma contemplan aquellas que por la naturaleza de sus operaciones podrían ver materializados riesgos operativos relacionados con TI que pueden exponer de forma significativa el sistema financiero y sus clientes.

Pasos de la Norma

Las entidades supervisadas, a partir de la entrada en vigencia del reglamento deben considerar siete pasos importantes a saber:

1. Remisión del Perfil y solicitud del tipo de gestión de TI.
2. Comunicación a la entidad del alcance de la auditoría externa.
3. Acreditación de la auditoría externa de TI.
4. Remisión del resultado de la auditoría externa de TI.
5. Comunicado del reporte del Supervisor.
6. Remisión del plan de acción.
7. Seguimiento y monitoreo.

Con la ejecución de dichos pasos se pretende que la entidad pueda establecer las prácticas de gestión que permitan perfeccionar el ambiente de control dentro de los plazos indicados.

Resultado esperado

Con la implementación de esta norma se espera que las entidades desarrollen la capacidad de gestionar TI y sus riesgos, con el objetivo de crear valor al negocio, lo anterior habilitando los siguientes aspectos:

Desde la óptica del negocio

1. Gobernabilidad de TI como parte del Gobierno corporativo para obtener valor y generar beneficios.
2. Armonizar, integrar y optimizar recursos, gestión de riesgos, así como prácticas y estándares internacionales.
3. Satisfacer los requerimientos de negocio (Partes interesadas).
4. Definir e implementar sistemas de gestión de calidad, mejora continua y documental basada en procesos.
5. Llevar TI a un lenguaje accesible para todo tipo de usuario.

Desde la óptica del supervisor

1. Evaluar la integración de los procesos de TI con los procesos y líneas de negocio y el logro de los objetivos de la entidad, para identificar el grado de dependencia tecnológica en sus operaciones.
2. Identificar los perfiles de riesgo en TI de los supervisados, con el propósito de concentrar esfuerzos en entidades con mayor exposición o con mayores debilidades de control.
3. Guiar a la alta administración, así como a los líderes o responsables de los procesos y líneas de negocio.

Título: ***Nueva regulación para la gestión de la Tecnologías de la Información (TI) para el sector financiero costarricense.***

Tema: ***Normativa de Tecnologías de Información para el Sistema Financiero Costarricense emitida por el CONASSIF.***

Propósito: ***Realizar un acercamiento al medio sobre los elementos más relevantes del reglamento de gestión de TI.***

Palabras clave: **Reglamento de Gestión de Tecnología de Información, Auditoría de TI, CONASSIF, Supervisión basada en riesgos; SUGEF, SUPEN, SUGEVAL; SUGESE, ISACA, COBIT, CISA.**

El autor:

El Ing. David Ricardo Rodríguez Calderón, es Lic. en Gestión de Recursos Tecnológicos, Master en Administración de Empresas con énfasis en Gerencia de Proyectos. CobiT 5 e ITIL Fundation Certificado por APMG.

Actualmente labora como Supervisor de Tecnologías de Información en la Superintendencia General de Seguros de Costa Rica, además es Profesor de la Catedra de TI de la Escuela de Administración de Negocios de la UCR, y realiza consultorías e implementación de CobiT e ITIL.

Incorporado al Colegio de Profesionales en Informática y Computación (CPIC) y a la Asociación de Auditoría y Control de los Sistemas de Información ISACA (Information Systems Audit and Control Association).

Cuenta con más de cinco años de experiencia implementando marcos de supervisión y control basado en mejores prácticas y estándares internacionales en el Banco Central de Costa Rica para la Superintendencia de General de Seguros (***Sugese***) y para la Superintendencia General de Entidades Financieras (***Sugef***).

Datos del contacto:

Teléfonos:
506 2243-5130
506 89259856

E-mail:
david.rodriguezcalderon@ucr.ac.cr
rodriguezcd@sugese.fi.cr
davidrrc@gmail.com

Ref. Reglamento General de Gestión de la Tecnología de la Información.

Publicado en el Alcance a la Gaceta No 80, del 17 de abril del 2017