SUGEF

SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS

Certificada con ISO-9001/2008

RESOLUCIÓN DEL SUPERINTENDENTE SUGEF-R-007-2010

SUGEF-R-007-2010. Superintendencia General de Entidades Financieras. Despacho de la Superintendencia General de Entidades Financieras, San Ana, a las catorce horas del 21 de julio de 2010.

Considerando que:

1. El Consejo Nacional de Supervisión del Sistema Financiero, mediante el Artículo 5 del Acta de la Sesión 853-2010 del 21 de mayo de 2010 aprobó varias modificaciones al Acuerdo SUGEF 14-09, "Reglamento sobre la Gestión de la Tecnología de Información", vigentes a partir del 15 de junio de 2010.
2. De conformidad con el artículo 4, 10, 13 y 14 del Reglamento indicado, corresponde al Superintendente General de Entidades Financieras emitir los contenidos, la forma y medio de remisión del Perfil Tecnológico de las entidades, las condiciones para la ejecución e informe de la auditoría externa de TI y el formato de presentación del Plan Correctivo–Preventivo requerido por la SUGEF ante las debilidades identificadas en la evaluación de TI.
3. Según el Artículo 131, inciso b) de la Ley Orgánica del Banco Central de Costa Rica, Ley N° 7558, corresponde al Superintendente General de Entidades Financieras tomar las medidas necesarias para ejecutar los acuerdos del Consejo Nacional de Supervisión.
4. La experiencia en la aplicación del Reglamento ha evidenciado la necesidad de ajustar el Formulario del Perfil Tecnológico; dichos ajustes procuran minimizar la incidencia de errores en el llenado de las tablas de información. Asimismo, con el propósito de coadyuvar con el proceso de documentación de la ejecución de la auditoría de TI y el control de calidad de la información, se introducen mejoras a la Matriz de Calificación de la Gestión de TI.

Dispone:

Modificar la Resolución del Superintendente SUGEF-R-839-2009 Lineamientos Generales para la aplicación del Reglamento sobre la Gestión de la Tecnología de Información, Acuerdo SUGEF 14-09", de conformidad con el texto que se adjunta.

Rige a partir de su comunicación.

Francisco Lay Solano
Superintendente General

OSC/JGTF/GSC/JLCH/gvl

Teléfono (506) 2243-4848
Facsimile (506) 2243-4849
Apartado 2762-1000
San José, Costa Rica
Correo electrónico:
sugefcr@sugef.fi.cr
Internet: www.sugef.fi.cr

A. FORMULARIO PERFIL TECNOLÓGICO

A.1 Descripción

El formulario del Perfil Tecnológico está compuesto por dieciocho tablas con campos predefinidos para completar por parte de la entidad. Mediante una guía complementaria se establecen las pautas a efecto de facilitar su llenado.

La estructura de dicho formulario se presenta a continuación:

Número de tabla	Detalle de la tabla
TABLA 1	Datos de identificación
TABLA 2	Procesos del marco para la gestión de TI
TABLA 3	Mapeo de procesos y subprocesos del negocio
TABLA 4	Organigrama(s) de la(s) entidad(es)
TABLA 5	Organigrama(s) de TI de la(s) entidad(es)
TABLA 6	Conformación del comité de TI
TABLA 7	Proveedores de TI
TABLA 8	Servicios de TI
TABLA 9	Inventario de tipos documentales
TABLA 10	Personal de TI
TABLA 11	Centros de cómputo (procesamiento y almacenamiento)
TABLA 12	Equipos de acceso, control físico y ambiental
TABLA 13	Inventario de equipo que soporta los servicios
TABLA 14	Sistemas de Información
TABLA 15	Software
TABLA 16	Proyectos de TI
TABLA 17	Planes de adquisición
TABLA 18	Servicios electrónicos

A.2 Plantilla del formulario

La SUGEF tendrá a disposición de las entidades un vínculo en su página WEB (www.sugef.fi.cr), mediante el cual las entidades pueden descargar el archivo electrónico del Formulario de Perfil Tecnológico y la guía complementaria. La ruta es la siguiente:

- Normativa/Normativa prudencial/Normativa vigente/Acuerdo SUGEF 14-09.

Alternativamente podrá utilizar las rutas siguientes:

- Perfil tecnológico
  http://www.sugef.fi.cr/servicios/documentos/Normativa/Reglamento%2014-09/SUGEF14-09-Reglamentacion.asp

- Guía complementaria para el perfil tecnológico
  http://www.sugef.fi.cr/servicios/documentos/Normativa/Reglamento%2014-09/SUGEF14-09-GuiasyManuales.asp

A.3 Mecanismo de remisión (medio y formato)

Las entidades deben remitir, en el formato liberado, la información del Perfil Tecnológico debidamente cumplimentada, en las fechas dispuestas conforme al Reglamento; para ello la entidad debe usar la aplicación SICVECA.

B. CONDICIONES PARA LA EJECUCIÓN E INFORME DE LA AUDITORÍA EXTERNA DE TI

B.1 Comunicación del alcance de la auditoría

El alcance de la auditoría será notificado a las entidades, según Artículos 11 y 12 del Reglamento. El comunicado del alcance de la auditoría incluye:

i. Explicación del alcance de auditoría basado en el marco referencial dispuesto en el artículo 9, los requerimientos generados del análisis del Perfil Tecnológico y otra información relacionada.
ii. Indicación para la descarga del archivo electrónico que contiene la "Matriz de Calificación de la Gestión de TI" con los procesos a evaluar.
iii. La fecha de remisión de los productos de la auditoría

B.2 Modalidad de la auditoría de TI

La auditoría consiste en obtener una conclusión sobre el cumplimiento de los objetivos de control y nivel de madurez asociados a cada proceso evaluado a partir de los requisitos establecidos por la versión 4.0 de CobiT. El trabajo ha de efectuarse en el contexto del marco dispuesto en el artículo 13 del Reglamento.

En lo concerniente a la expresión de la conclusión, esta puede emitirse de forma positiva o negativa según sea apropiado, respecto al cumplimiento de los objetivos de control y nivel de madurez para cada proceso evaluado.

El auditor debe brindar como producto de la auditoría:

i. Un Informe de auditoría con conclusiones.
ii. La Matriz de Calificación de la Gestión de TI debidamente cumplimentada.
iii. Una presentación de salida.

La ejecución de la auditoría externa de TI se rige por las guías y criterios profesionales que rigen en la materia, utilizando los "Estándares de TI, guías, herramientas y técnicas para auditoría, aseguramiento y control profesional" emitido por ISACA en el documento "IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals".

La presentación de salida consistirá en una exposición ejecutiva del Informe, y debe efectuarse en un plazo no mayor a 5 días hábiles posteriores a la fecha de la entrega de los productos de la auditoría. En dicha presentación participarán al menos dos funcionarios de la SUGEF previa convocatoria por parte de la entidad.

B.3 Control de calidad

El auditor como requisito previo debe atender las normas dispuestas por ISACA relacionadas con la ejecución de la auditoría e informe, S7 y G20, así como utilizar aquellas aplicables en razón del carácter y naturaleza del encargo.

En la ejecución de la auditoría debe contar con políticas y procedimientos que permitan verificar de manera adecuada que la conclusiones expresadas respecto a los objetivos de control y su cumplimiento son basadas en un escrutinio riguroso de la evidencia con el propósito de evitar sustentarlas en meras presunciones o afirmaciones.

B.4 Documentación

Es responsabilidad de cada entidad mantener actualizada y a disposición de SUGEF y del auditor externo de TI, la lista dispuesta en la Tabla B.4.1. "Índice de documentación"

Es responsabilidad del auditor externo de TI verificar la vigencia de la información listada en la tabla indicada.

Asimismo es responsabilidad del auditor externo de TI suministrar, como anexo al informe de auditoría, la Tabla B.4.1. "Índice de documentación" con la inclusión de otra documentación que haya sido recopilada durante la ejecución de la auditoría, a la cual debe asignarle un código de referencia y el nombre o descripción que corresponda.

Para los efectos, el auditor debe:

i. Velar porque el listado este completo, debidamente codificado y detallado, incluyendo la documentación recopilada durante la ejecución de la auditoría.
ii. Incluir, cuando se requiera, una referencia a la información contenida en el Perfil Tecnológico, para lo cual debe indicarse el número de la tabla en el campo de "detalle de documento".
iii. Verificar que el código asignado sea el mismo al que se hace referencia en la Matriz de Calificación de la Gestión de TI y/o en el informe.

Tabla B.4.1. Índice de documentación

Código	Detalle del documento
D-01	Perfil Tecnológico remitido a SUGEF.
Ejemplo: *D-01-Tabla-04 Organigramas de las entidades.* *D-01-Tabla-05 Organigramas de TI.* *D-01-Tabla-nn*	
D-02	Plan Estratégico de Tecnologías de Información.
D-03	Políticas, procedimientos e instructivos de Tecnologías de Información. Se debe incluir la política de seguridad de la organización.
Ejemplo: *D-03-001 Política de seguridad* *D-03-002 Procedimiento de ingreso y salida de equipos de cómputo.* *D-03-nnn*	
D-04	Plan Operativo Anual de Tecnologías de Información.
D-05	Cartera de Proyectos de Tecnología de Información y / o cronogramas de actividades de los diferentes proyectos de Tecnología de Información.
D-06	Manual de Puestos de Tecnología de Información.
D-07	Presupuesto de Tecnologías de Información.
D-08	Actas, minutas, oficios del Comité de TI y de los diferentes grupos de trabajo relacionados con Tecnología de Información.
D-09	Contratos de servicios, productos, convenios, así como los acuerdos con terceros (UC), acuerdos a nivel de servicio (SLA), acuerdos a nivel operativos (OLA).
D-10	Metodología y estándares relacionados a Tecnologías de Información.
D-11	Manuales de Tecnologías de Información (usuario, técnicos, operación, sistema, etc.)
D-12	Modelo de Arquitectura de Información, esquemas de seguridad implementados en los sistemas, bases de datos y sistemas operativos (lógico).

D-13	Registros o formularios de control usados para las diferentes actividades en Tecnología de Información.
D-14	Inventario de software, con detalle de licencia.- Tabla No. 14 del perfil tecnológico
D-15	Inventario de hardware, detallado por equipo, donde se indique el responsable de equipo. - Tabla No. 13 del perfil tecnológico
D-16	Documentación de las bases de datos con sus respectivos diagramas de entidad de relación.
D-17	Documentación de Roles y Perfiles de acceso de usuarios, grupos de trabajo, entre otros, que contemple la descripción detallada de roles, la documentación técnica de los roles, la descripción detallada de los perfiles y la documentación técnica de los perfiles.
D-18	Listado de usuarios, con el detalle de nombre y accesos autorizados. (Para sistemas de red, sistemas de aplicación y bases de datos).
D-19	Documentación sobre la configuración, mantenimiento y operación de las redes LAN, MAN o WAN (físico y lógico).
D-20	Pólizas de seguros de equipos electrónicos.
D-21	Plan de continuidad y contingencia.
D-22	Pruebas realizadas a los sistemas de comunicación, que validen la seguridad de entrada y salida de los datos, que contemplen los planes de pruebas seguridad y los planes de pruebas de sistemas.
D-23	Plan de capacitación en Tecnologías de Información usuario final y plan de capacitación para personal de Tecnologías de Información.
D-24	Evaluación del cumplimiento de los planes operativos.
D-25	Reportes de monitoreo realizado por el DBA, (tunning, valoración de índices, entre otros).

B.4 Descripción General de la Matriz de Calificación de la Gestión de TI

La Matriz de Calificación de la Gestión de TI es el instrumento para determinar el grado de cumplimiento de los objetivos de control y el nivel de madurez para cada proceso evaluado del marco para la gestión de TI de la entidad; dicho instrumento debe ser completado por el Auditor Externo de TI.

B.5. Plantilla de la Matriz de Calificación de la Gestión de TI

La Matriz de Calificación de la Gestión de TI está diseñada en forma de criterios de evaluación, dónde se establece un conjunto de enunciados sobre los objetivos de control detallados y los niveles de madurez de CobiT.

Los enunciados que plantea la matriz son de respuesta cerrada: **Sí, No y No Aplica (NA)** y para cada una se debe incluir la referencia a la documentación utilizada como evidencia, las técnicas de auditoría utilizadas, descripción de las pruebas de cumplimiento y sustantivas efectuadas, así como las observaciones y conclusiones pertinentes.

En la referencias debe indicar el código, dispuesto según la TABLA.B.4.1 Índice de documentación.

La SUGEF tendrá a disposición de las entidades y los auditores externos un vínculo en su página WEB

(www.sugef.fi.cr), mediante el cual se puede descargar el archivo electrónico de la Matriz de Calificación de la Gestión de TI y una guía con las pautas para completarlo, según la ruta siguiente:

- Normativa/Normativa prudencial/Normativa vigente/Acuerdo SUGEF 14-09.

Alternativamente podrá copiar las rutas siguientes:

- Matriz de Calificación de la Gestión de TI
  http://www.sugef.fi.cr/servicios/documentos/Normativa/Reglamento%2014-09/SUGEF14-09-Reglamentacion.asp

- Guía para completar la Matriz de Calificación de la Gestión de TI
  http://www.sugef.fi.cr/servicios/documentos/Normativa/Reglamento%2014-09/SUGEF14-09-GuiasyManuales.asp

B.6 Mecanismo de remisión (medio y formato)

Las entidades, deben remitir la información de la Matriz de Calificación de la Gestión de TI debidamente cumplimentada, junto con el informe y los anexos correspondientes de la auditoría externa de TI entregados por el auditor externo; dentro del plazo establecido en la notificación del alcance de la auditoría externa, para ello la entidad debe usar la aplicación SICVECA.

C. PLAN CORRECTIVO / PREVENTIVO

C.1 Descripción General

El Plan Correctivo / Preventivo es un producto entregable por la entidad para indicar las acciones a seguir con el fin de corregir y/o prevenir incumplimientos, debilidades y/o hallazgos encontrados en la ejecución de la Auditoría Externa de TI. Este producto será remitido por la entidad según solicitud previa de la SUGEF siguiendo las pautas establecidas en el punto C2.

C2. Plantilla del Plan Correctivo / Preventivo

La SUGEF tendrá a disposición de las entidades y los auditores externos un vínculo en su página WEB (www.sugef.fi.cr), mediante el cual se puede descargar el archivo electrónico del Plan correctivo / preventivo y una guía donde se establecen las pautas para completarlo, según la ruta siguiente:

- Normativa/Normativa prudencial/Normativa vigente/Acuerdo SUGEF 14-09.

Alternativamente podrá copiar las rutas siguientes:

- Plan correctivo / preventivo:
  http://www.sugef.fi.cr/servicios/documentos/Normativa/Reglamento%2014-09/SUGEF14-09-Reglamentacion.asp
- Guía para completar el plan correctivo preventivo:
  http://www.sugef.fi.cr/servicios/documentos/Normativa/Reglamento%2014-09/SUGEF14-09-GuiasyManuales.asp

C.3 Mecanismo de remisión (Medio y formato)

Las entidades deben remitir, la información del Plan Correctivo / Preventivo, debidamente cumplimentada, para ello la entidad debe usar la aplicación SICVECA.

D. ANEXOS

El Perfil Tecnológico, la Matriz de Calificación de la Gestión de TI y el Formato del Plan correctivo / preventivo se puede accesar en el sitio WEB de la SUGEF, la ruta es la siguiente:

- Normativa/Normativa prudencial/Normativa vigente/Acuerdo SUGEF 14-09/Formularios y Guías.