SUGEF

SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS

Certificada con ISO-9001/2008

RESOLUCIÓN DEL SUPERINTENDENTE SUGEF-R-001-2011

SUGEF-R-001-2011. Superintendencia General de Entidades Financieras. Despacho de la Superintendencia General de Entidades Financieras, San Ana, a las doce horas del veinticuatro de enero del 2011.

Considerando que:

1. El artículo 4 del Acuerdo SUGEF 14-09, "Reglamento sobre la Gestión de la Tecnología de Información", faculta al Superintendente General de Entidades Financieras para emitir los lineamientos generales para aplicación del citado reglamento.
2. El Sistema de captura, verificación y carga de datos (SICVECA) provee de una plataforma tecnológica desarrollada por la Superintendencia, para el envío y la recepción de información de las entidades financieras.
3. En congruencia con la mejora continua en sus procesos, la Superintendencia ha incorporado al Manual de Información SICVECA la Clase de Datos 24 (Perfil Tecnológico), mediante la cual se pone a disposición de las entidades los formularios que generan los archivos XML específicos del perfil tecnológico.
4. Con la implementación de esta aplicación automatizada se procura una mejora en la eficiencia del proceso y en la calidad de la información que se envía a SUGEF, por medio de validaciones que se incorporan tanto en los formularios del perfil tecnológico, como las ya existentes en la aplicación SICVECA. Asimismo contribuye a la preparación y registro de la información por parte de las entidades.

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

OSCH/GTI/GSC/[illegible]/gm*

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

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"

A. FORMULARIOS DEL PERFIL TECNOLÓGICO

Los formularios del Perfil Tecnológico son una serie plantillas compuestas por campos predefinidos para completar por parte de la entidad, publicados en la página www.sugef.fi.cr en la ruta:

> Normativa> Manual de Información SICVECA >Opción "Acuerdo 14-09".

Para el llenado de los formularios del perfil tecnológico se dispone de una "Guía para completar el perfil tecnológico", la cual contiene las pautas que facilitan el entendimiento de la estructura de los formularios, así como los pasos a seguir para descargar, llenar y remitir dicha información a la Superintendencia. La guía se ubica en la ruta:

> Normativa> Manual de Información SICVECA >Opción "Acuerdo 14-09"> "Formularios y guías"

B. 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 del marco para la gestión de TI de la entidad; dicha matriz es liberada por medio de SICVECA a la entidad cuando SUGEF notifica el alcance de la auditoría.

La matriz de calificación de la gestión de TI, está diseñada en forma de criterios de evaluación donde se establecen un conjunto de enunciados sobre los objetivos de control detallados y los niveles de madurez de CobiT.

La entidad debe utilizar la "Guía para descargar la matriz de calificación de la gestión de TI" que contiene los pasos requeridos para obtener dicha matriz. El Auditor CISA debe utilizar la "Guía para completar la matriz de calificación de la gestión de TI" la cual contiene las pautas que facilitan el entendimiento de la estructura de la matriz de calificación de la gestión de TI. Las guías se ubican en la ruta:

> Normativa> Manual de Información SICVECA >Opción "Acuerdo 14-09"> "Formularios y guías"

C. PLAN CORRECTIVO / PREVENTIVO

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 debe ser remitido por la entidad según solicitud previa de la SUGEF.

La entidad debe utilizar la "Guía para completar el Plan Correctivo / Preventivo, el cual contiene las instrucciones para llenar y remitir dicho plan a la SUGEF. La guía se ubica en la ruta:

> Normativa> Manual de Información SICVECA >Opción "Acuerdo 14-09"> "Formularios y guías"

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

D.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*

D.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.

D.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.

D.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 D.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).*

Rige a partir de su comunicación