RESOLUCIÓN DEL SUPERINTENDENTE SUGEF-R-839-2009

SUGEF-R-839-2009. Superintendencia General de Entidades Financieras. Despacho del Superintendente General de Entidades Financieras, a las 9:40 horas del 06 de marzo de 2009.

Considerando:

1. Que el Consejo Nacional de Supervisión del Sistema Financiero, mediante el Artículo 6 del Acta de la Sesión 773-2009 del 20 de febrero de 2009 aprobó el Acuerdo SUGEF 14-09, denominado "Reglamento sobre la Gestión de la Tecnología de Información",
2. Que de conformidad con el artículo 4 del reglamento indicado, corresponde al Superintendente General de Entidades Financieras emitir los contenidos del Perfil Tecnológico de las entidades, las condiciones para la ejecución 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. Que de conformidad con 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.

Dispone:

Emitir los siguientes 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.

José Armando Fallas Martínez
Superintendente General a.i.

GTP/GSC/JCCM/lsd*

LINEAMIENTOS PARA LA APLICACIÓN DEL REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN ACUERDO SUGEF 14-09

A. FORMULARIO PERFIL TECNOLÓGICO

TABLA DE CONTENIDO

TABLA 1 Datos de Identificación de la Entidad	
Fecha:	
Nombre de Entidad:	
Dirección:	
Teléfono:	
Persona de Contacto (TI):	
Cargo:	
E-mail:	

TABLA 2 Procesos del Marco para la Gestión de TI		
Aprobación	**<Indique el acuerdo de Junta Directiva o autoridad equivalente mediante la cual se aprueba el marco para la gestión de TI de la entidad>**	Marco para la gestión TI
DOMINIO	Procesos COBIT® 4.0	Selección[1]
Planear y Organizar	PO1 Definir un Plan Estratégico de TI	☐
	PO2 Definir la Arquitectura de la Información	☐
	PO3 Determinar la Dirección Tecnológica	☐
	PO4 Definir los Procesos, Organización y Relaciones de TI	☐
	PO5 Administrar la Inversión en TI	☐
	PO6 Comunicar las aspiraciones y la dirección de la gerencia	☐
	PO7 Administrar los Recursos Humanos de TI	☐
	PO8 Administrar la Calidad	☐
	PO9 Evaluar y administrar los riesgos TI	☐
	PO10 Administrar Proyectos	
Adquirir e Implantar	AI1 Identificar Soluciones Automatizadas	☐
	AI2 Adquirir y Mantener Software Aplicativo	☐
	AI3 Adquirir y Mantener Infraestructura Tecnológica	☐
	AI4 Facilitar la Operación y el Uso	☐
	AI5 Adquirir Recursos de TI	☐
	AI6 Administrar Cambios	☐
	AI7 Instalar y Acreditar Soluciones y Cambios	☐
Entregar y Dar Soporte	DS1 Definir y Administrar los Niveles de Servicio	☐
	DS2 Administrar los servicios de terceros	☐
	DS3 Administrar el Desempeño y la Capacidad	☐
	DS4 Garantizar la continuidad del Servicio	☐
	DS5 Garantizar la Seguridad de los Sistemas	☐
	DS6 Identificar y Asignar Costos	☐
	DS7 Educar y Entrenar a los Usuarios	☐
	DS8 Administrar la mesa de Servicio y los Incidentes	☐
	DS9 Administrar la Configuración	☐
	DS10 Administrar los Problemas	☐
	DS11 Administrar los Datos	☐
	DS12 Administrar el Ambiente Físico	☐
	DS13 Administrar las Operaciones	☐
Monitorear y Evaluar	ME1 Monitorear y Evaluar el Desempeño de TI	☐
	ME2 Monitorear y Evaluar de Control Interno	☐
	ME3 Garantizar el cumplimiento regulatorio	☐
	ME4 Proporcionar Gobierno de TI	☐

Nota:

1 Seleccione los procesos que le aplican a la entidad, considerando los procesos definidos como obligatorios y opcionales según el Artículo 6 del Acuerdo SUGEF 14-09.

TABLA 3 Mapeo de procesos críticos del negocio						
Proceso[1]	**Subproceso**	**Descripción**[2]	**Responsable**[3]	**Dependencia tecnológica**[4]	**Soporte**[5]	**Identificador**[6]
Proceso A	Subproceso A.1					
	Subproceso A.2					
Proceso ...n						

Notas:

[1] Enumere cada uno de los procesos (y subprocesos) del negocio que se articulan para lograr los objetivos de la entidad. Se sugiere que la determinación de procesos y subprocesos sea establecida considerando los criterios de La Organización Internacional para la Estandarización o ISO (en inglés, International Organization for Standardization) o La Asignación de las Líneas de Negocio del documento "Convergencia Internacional de medidas y normas de Capital" del Comité de Supervisión Bancaria de Basilea (2004).

[2] Indicación breve de la naturaleza y objetivo del subproceso. Debe indicarse si corresponde a back office o front office (considerando si hay una relación directa o no con los clientes).

[3] Nombre de la Unidad o persona en quien recae la responsabilidad y rendición de cuentas.

[4] El grado de dependencia tecnológica representa la relación de subordinación y sensibilización de los procesos de negocio, con respecto a la información y la tecnología que le soporta. Deberá calificarse según las siguientes categorías:

GRADO	DESCRIPCIÓN
Mínimo	Menos del 20% de las actividades del proceso, relacionadas con captura, almacenamiento, transformación, transmisión y presentación se encuentran soportadas por tecnologías de información.
Parcial Bajo	Más del 20% pero menos del 50% de las actividades del proceso, relacionadas con captura, almacenamiento, transformación, transmisión y presentación se encuentran soportadas por tecnologías de información.
Parcial Alto	Más del 50% pero menos del 75% de las actividades del proceso, relacionadas con captura, almacenamiento, transformación, transmisión y presentación se encuentran soportadas por tecnologías de información.
Total	Más del 75% de las actividades del proceso, relacionadas con captura, almacenamiento, transformación, transmisión y presentación se encuentran soportadas por tecnologías de información.

[5] Asigne la letra que identifica el tipo de soporte, puede incluir más de una letra, según la siguiente correspondencia:

IDENTIFICACION	TIPO DE SOPORTE	DESCRIPCIÓN
A	Aplicaciones	Corresponden a Hojas de cálculo electrónicas, procesadores de texto, etc.…
B	Sistemas de soporte a nivel operativo	Corresponden a sistemas transaccionales o sistemas de procesamiento de transacciones TPS por sus siglas en inglés (Transaction Processing System)
C	Sistemas de soporte a nivel de Conocimiento	Corresponden a sistemas para automatización de Oficinas, Trabajo y Conocimiento. KWS, knowledge work system, o sistema de manejo de conocimiento
D	Sistemas de soporte a nivel Gerencial	Corresponde a Sistemas de apoyo a ejecutivo, de soporte a las Decisiones y Gestión de Riesgos. ESS, executive support system, o sistemas de apoyo a ejecutivos
E	Sistemas de soporte a nivel Estratégico	Corresponden a sistema expertos para pronósticos o simulaciones

[6] Defina un código que permite identificar el subproceso y proceso, a modo de ejemplo para la tabla el identificador del proceso A y suproceso A.1 será P-A-1.

TABLA 4 Composición del Comité de TI				
Nombre	**Puesto que desempeña en la organización**	**Cargo dentro del Comité**	**Periodo**	**Nombramiento[1]**
…				

Nota:
[1]Indique el acuerdo de Junta Directiva o autoridad equivalente mediante la cual se nombra en el cargo.

TABLA 4.1 Organigrama Institucional

El organigrama debe mostrar la ubicación del departamento o unidad de informática dentro de la entidad.

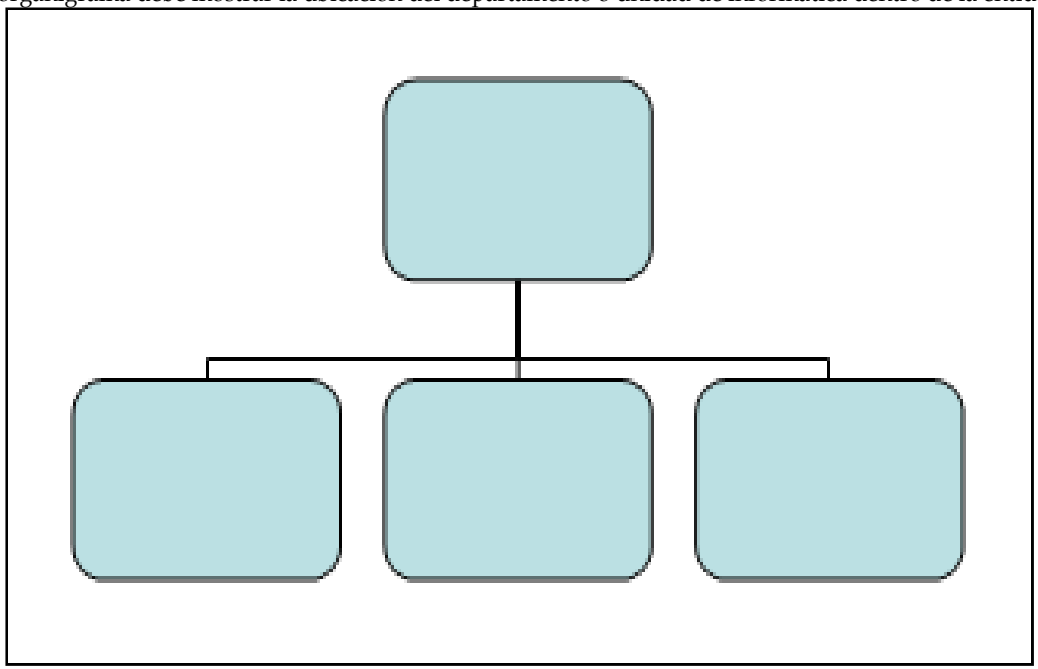

TABLA 4.2 Organigrama del Departamento de TI

El organigrama debe mostrar la distribución formal de responsabilidades en el departamento o unidad de informática.

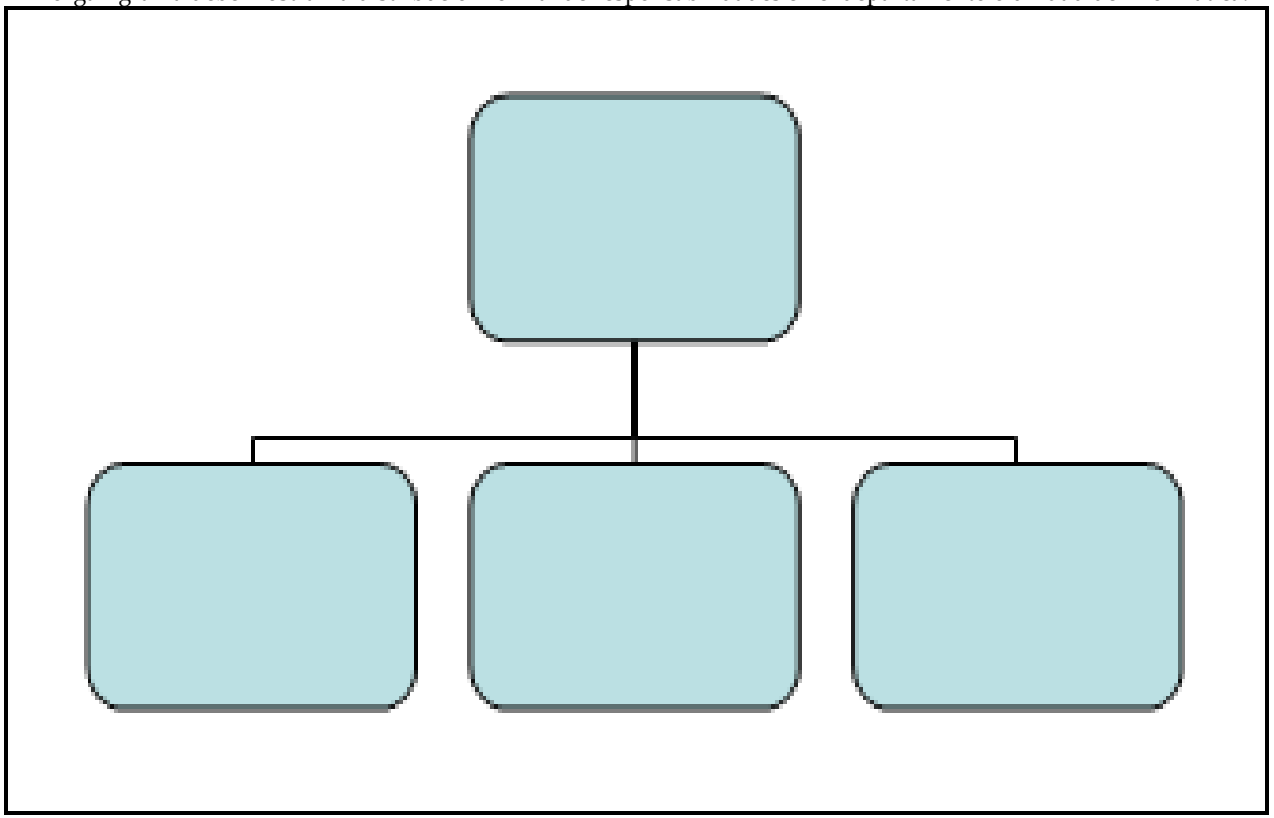

TABLA 5 Servicios de TI														
Nombre del servicio	**Provisto por TI de la entidad**	**Provisto por terceros a la entidad (Tercerización)**												
	S/N	**Empresa que presta el Servicio**[1]	**País** [2]	**Registro** [3]	**Nombre del Contacto**	**Teléfono**	**E-mail**	**Nivel de delegación Tipo (P/D/M)**[4]	**Vencimiento** [5]	**Proceso Asociado**[6]	**Supervisión o Control** [7]			
											S/N	**Periodicidad**	**Revisor**	**Estándar**
…														

Notas:

Utilice una línea por cada servicio. Si TI de la entidad brinda el servicio indique S(si), de lo contrario indique N (no), y complete lo correspondiente a apartado de Tercerización. La siguiente es una lista no exhaustiva de los servicios:

Auditoría de sistemas	Seguridad de la información	Administración de la Calidad de TI	Administración del Riesgo de TI
Administración de Incidentes y Mesa de ayuda	Administración de Cambios	Administración de Versiones	Administración de Configuración
Administración de Niveles de Servicio	Administración de problemas	Conexión -Conectividad	Conexión con red SWIFT
Conexión Bcos Corresponsales	Banca Electrónica	Interconexión con los centros de negocio (sucursales, agencias, oficinas, etc)	Red de cajeros electrónicos
Administración Tarjetas de crédito	Soporte usuarios finales	Programación	Administración de resguardos
Implementaciones de sistemas	Administración de bases de datos	Administración de redes	Conexión Internet
Administración sistemas operativos	Asignación de perfiles y accesos		…

1 Corresponde al nombre comercial del proveedor.

2 Nombre del país en donde se ubica el proveedor.

3 Cédula jurídica o identificación según corresponda.

4 **Tipo: P =** Procesamiento **D =** Desarrollo **M**= Mantenimiento. (Puede indicarse más de una letra diferente).

5 Fecha de vencimiento del contrato o periodo cubierto.

6 Corresponde al código definido en la tabla 3 (celda identificador).
7 Indique si la empresa es sujeta a revisiones y/o auditorias (S para sí y N para no), la periodicidad y el nombre de quien la efectúa, así como el estándar utilizado. En el caso de que el proveedor del servicio sea una entidad supervisada, la entidad deberá adjuntar una certificación expedida por el organismo supervisor, en la que se indique si tiene conocimiento de la prestación de este tipo de servicios y especificar si las mismas son sujetas de supervisión de manera regular.

TABLA 6 Personal Clave de TI					
Tipo de servicio*1*	**Nombre**	**Dependencia funcional** *2*	**Teléfono**	**Cargo**	**E-mail**
Otros…					

Notas:
El o los nombres que se asignen son aquellos en quien(es) recae la responsabilidad y rendición de cuentas. El área de TI debe presentar una clara separación de funciones incompatibles, con el propósito de evitar conflictos de interés.
1 Corresponde a los mismos servicios identificados en la tabla 5.
2 Gerencia, Departamento o unidad a la que pertenece.

TABLA 7 Centros de Cómputo			
N°	*Ubicación física (geográfica)*	**Funge como Sitio Alterno Sí/No**	**Cantidad de oficinas o centros de negocio que dependen del centro de cómputo**
…			

Notas:
Se considera de manera general que un Centro de Cómputo es el conjunto de recursos físicos, lógicos y humanos necesarios para la organización, ejecución y control de las actividades informáticas.

TABLA 8 Aplicaciones o Sistemas en Desarrollo o por Implantarse						
Proceso que apoya*1*		**Descripción del Sistema**	**Desarrollador**	**Inversión Aproximada ($)**	**Fechas Estimadas**	
					Desarrollo	**Implantación**
Proceso de Negocio	Proceso COBIT					
...						

Nota:
1 Indique el proceso de Cobit o de negocio que apoya. Para los procesos del negocio utilice el código definido en la tabla 3 (celda identificador).

TABLA 9 Aplicaciones Existentes									
Tipo de Soporte*1*	**Proceso Asociado*2***	**Fecha Implantación**	**Internet (S/N)*3***	**Nombre herramienta *4***	**Base de Datos Utilizada*5***	**Tipo de Desarrollo*6***	**Empresa Desarrolladora**	**Código Fuente*7***	**Equipo Utilizado*8***
...									

Notas:

*1*Letra que identifica el tipo de soporte, puede incluir más de una letra, según la siguiente correspondencia:

ID	TIPO DE SOPORTE	DESCRIPCION
A	Aplicaciones	Corresponden a Hojas de cálculo electrónicas, procesadores de texto, etc.…
B	Sistemas de soporte a nivel operativo	Corresponden a sistemas transaccionales o sistemas de procesamiento de transacciones TPS por sus siglas en inglés (Transaction Processing System)
C	Sistemas de soporte a nivel de Conocimiento	Corresponden a sistemas para automatización de Oficinas, Trabajo y Conocimiento. KWS, knowledge work system, o sistema de manejo de conocimiento
D	Sistemas de soporte a nivel Gerencial	Corresponde a Sistemas de apoyo a ejecutivo, de soporte a las Decisiones y Gestión de Riesgos. ESS, executive support system, o sistemas de apoyo a ejecutivos
E	Sistemas de soporte a nivel Estratégico	Corresponden a sistema expertos para pronósticos o simulaciones

2 Corresponde al código definido en la tabla 3 (celda identificador).

3 **S=** Si se puede acceder la aplicación mediante Internet, **N=** No se puede acceder la aplicación mediante Internet.

4 Incluir el nombre de la herramienta de desarrollo y la versión.

5 Incluir el nombre del motor de la base de datos y la versión.

6 **Propio=** Realizado en Casa, **Contratado=** Hecho a la medida por Empresa Desarrolladora,
Paquete= Comprado a Empresa Desarrolladora, **Alquilado=** Pago de Alquiler por el uso de la aplicación.

7 **S=** Si posee el código fuente, **N=** No posee código fuente.

8 Equipo o Servidor en el que está corriendo la aplicación.

TABLA 10 Inventario del equipo que soporta los servicios

Proceso Asociado*1*	**Centro de Computo***2*	**Hardware** *3*	**Marca - Modelo**	**Ambiente** *4*	**Proveedor**	**Cantidad**	**Leasing S/N**	**Fecha de adquisición o periodo cubierto**	**Contrato de Soporte** *6*	**Garantía***7*
…										

TABLA 11 Planes para adquirir equipo que soporta los servicios

Proceso Asociado*1*	**Centro de Computo***2*	**Hardware** *3*	**Marca - Modelo**	**Ambiente** *4*	**Proveedor**	**Cantidad**	**Leasing S/N**	**Fecha de adquisición o periodo cubierto**	**Contrato de Soporte** *6*	**Garantía***7*	**Fecha estimada**
…											

Notas tabla 10 y 11:

*1*Corresponde al código definido en la tabla 3 (celda identificador).
2 Identifique con el mismo número asignado que en la tabla 7.
3 Incluir el equipo que soporta los servicios, según sean: Servidores, Ruteadores, Hubbs, Switches, UPSs).
4 **P=** Producción, **D=** Desarrollo, **U=** Pruebas.
5 Indique si el equipo es arrendado (leasing).
6 **S=** Si cuenta con contrato de soporte VIGENTE, **N=** No cuenta con contrato de soporte o bien el mismo ya expiró.
7 **S=** Si cuenta con garantía VIGENTE, **N=** No cuenta con garantía o bien la misma ya expiró.

TABLA 12 Ambiente de Procesamiento (Equipo de soporte de operaciones y control ambiental)							
Equipo*1*	**Marca**	**Modelo**	**Proveedor**	**Cantidad**	**Fecha de Adquisición**	**Contrato de Soporte*2***	**Garantía*3***
…							

TABLA 13 Planes para adquirir equipo de soporte de operaciones y control ambiental							
Equipo	**Marca**	**Modelo**	**Proveedor**	**Cantidad**	**Fechas Estimadas**		**Inversión Aproximada ($)**
					Adquisición	**Implantación**	
…							

Notas tabla 12 y 13:
1 Incluir el equipo de monitoreo tales como detectores de humedad, sensores de movimiento, detectores de humo, aire acondicionado, planta de energía, cámaras de circuito cerrado de televisión, etc.
2 **S=** Si cuenta con contrato de soporte VIGENTE, **N=** No cuenta con contrato de soporte o bien el mismo ya expiró.
3 **S=** Si cuenta con garantía VIGENTE, **N=** No cuenta con garantía o bien la misma ya expiró.

TABLA 14 Banca electrónica								
Servicio	**[1] S/N**	**Red administrada por**		**conexión en línea directa (on-line)[2]**	**Interrupción [3]**	**Comunicación de las condiciones legales y operativas [4]**	**Autenticación[5]**	**Plan de continuidad[6]**
		Entidad	**Proveedor**					
Cajeros automáticos								
Puntos de Venta								
(e-banking).								
Banca Móvil (m-Banking)[7]								
Otros, específique								

Notas:

[1] S= SI provee este servicio N= no provee este servicio.

[2] Debe indicarse si el servicio opera en un esquema de proceso en tiempo real y conexión en línea directa con el computador que administra la red y la base de datos que opera.

[3] En caso de interrupción, indique si el dispositivo o servicio queda fuera de servicio para todo tipo de transacciones hasta la normalización del proceso.

[4] Indicar que medio utiliza la entidad para establecer y comunicar a sus clientes las condiciones legales y operativas bajo las cuales se brindará el servicio financiero, por ejemplo mediante contrato de adhesión o publicación de reglamentos.

[5] Indicar las medidas de autenticación que utilizan para verificar la identidad de cada uno de los usuarios a los que preste sus servicios, así como los tipos de servicios de operaciones por Internet que cada uno de ellos tiene autorizado realizar.

[6] Indicar si la entidad cuenta con un plan específico de continuidad del servicio.

[7] Corresponde a transacciones cursadas por medio de dispositivos móviles, que utilicen comunicaciones de telefonía celular o de redes inalámbricas.

TABLA 15 Aplicaciones Existentes S/ Legitimación de Capitales									
Tipo de Soporte[1]	**Proceso Asociado[2]**	**Fecha Implantación**	**Internet (S/N)[3]**	**Nombre herramienta [4]**	**Base de Datos Utilizada[5]**	**Tipo de Desarrollo[6]**	**Empresa Desarrolladora**	**Código Fuente[7]**	**Equipo Utilizado[8]**
…									

Notas:

El propósito es identificar las aplicaciones, controles o rutinas de alerta que permitan evitar que los servicios de la entidad sean utilizados para legitimar capitales provenientes de actividades ilícitas.

[1]Letra que identifica el tipo de soporte, puede incluir más de una letra, según la siguiente correspondencia:

ID	TIPO DE SOPORTE	DESCRIPCION
A	Aplicaciones	Corresponden a Hojas de cálculo electrónicas, procesadores de texto, etc.…
B	Sistemas de soporte a nivel operativo	Corresponden a sistemas transaccionales o sistemas de procesamiento de transacciones TPS por sus siglas en inglés (Transaction Processing System)
C	Sistemas de soporte a nivel de Conocimiento	Corresponden a sistemas para automatización de Oficinas, Trabajo y Conocimiento. KWS, knowledge work system, o sistema de manejo de conocimiento
D	Sistemas de soporte a nivel Gerencial	Corresponde a Sistemas de apoyo a ejecutivo, de soporte a las Decisiones y Gestión de Riesgos. ESS, executive support system, o sistemas de apoyo a ejecutivos
E	Sistemas de soporte a nivel Estratégico	Corresponden a sistema expertos para pronósticos o simulaciones

[2] Corresponde al código definido en la tabla 3 (celda identificador).

[3] **S=** Si se puede acceder la aplicación mediante Internet, **N=** No se puede acceder la aplicación mediante Internet.

[4] Incluir el nombre de la herramienta y la versión.

[5] Incluir el nombre del motor de la base de datos y la versión.

[6] **Propio=** Realizado en Casa, **Contratado=** Hecho a la medida por Empresa Desarrolladora,
Paquete= Comprado a Empresa Desarrolladora, **Alquilado=** Pago de Alquiler por el uso de la aplicación.

[7] **S=** Si posee el código fuente, **N=** No posee código fuente.

[8] Equipo o Servidor en el que está corriendo la aplicación.

LINEAMIENTOS PARA LA APLICACIÓN DEL REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN ACUERDO SUGEF 14-09

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

Esta guía tiene como objeto establecer los lineamientos generales que deben atenderse en la ejecución de la auditoría externa.

A. Modalidad de auditoría de TI

La auditoría consiste en un Trabajo para Atestiguar, cuyo propósito es 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:

1. Un Informe con conclusiones,
2. La Matriz de Calificación de la Gestión de TI debidamente cumplimentada y;
3. Una presentación de salida.

El informe deberá ajustarse a los contenidos dispuestos por la NITA 3000.
La matriz de calificación de la Gestión de TI deberá ser remitida de manera conjunta con el Informe. En el literal D se establece la metodología para completar la matriz.
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 asignada a la entidad para remitir los productos de la auditoría. En dicha presentación participarán al menos dos funcionarios de la SUGEF previa convocatoria por parte de la entidad.

B. Control de calidad

El auditor como requisito previo debe cumplir -en lo procedente- con los requisitos dispuestos por la Norma Internacional de Control de Calidad 1 (NICC 1); 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.

C. Documentación y reportes mínimos

Es responsabilidad de cada entidad mantener a disposición de la SUGEF y del auditor independiente, la siguiente lista no exhaustiva de documentos y/o reportes. Es responsabilidad del auditor independiente, previo al inicio de la auditoría de TI, verificar que la información que se detalla se mantiene vigente.

Código	Detalle
D-001	Perfil Tecnológico remitido a SUGEF.
D-002	Plan Estratégico de Tecnología de Información.
D-003	Políticas y procedimientos formalmente documentados sobre Tecnología de Información.
D-004	Organigrama detallado del departamento de T.I.
D-005	Plan de trabajo anual.
D-006	Cronograma de actividades de los diferentes proyectos en Tecnología de información.
D-007	Manual de Puestos de Tecnología de Información.
D-008	Copia del Presupuesto para T.I.
D-009	Actas, minutas, oficios del Comité de TI y de los diferentes grupos de trabajo relacionados con Tecnología de Información.
D-010	Copia de contratos de servicios, productos, convenios, etc.
D-011	Metodología y estándares para el desarrollo y mantenimiento de sistemas de información.
D-012	Manuales de usuario, técnicos y de operación de los diferentes sistemas.
D-013	Esquemas de seguridad implementados en los sistemas, bases de datos y sistemas operativos.
D-014	Copia de los formularios de control usados para las diferentes actividades en Tecnología de Información.
D-015	Inventario de software, con detalle de licencia.
D-016	Inventario de hardware, detallado por equipo, responsable de equipo (si aplica).
D-017	Documentación de las bases de datos con sus respectivos diagramas de entidad de relación.
D-018	Documentación de Perfiles de acceso de usuarios, grupos de trabajo, entre otros
D-019	Listado de usuarios, con el detalle de nombre y accesos autorizados. (Para sistemas de red y sistemas de aplicación).
D-020	Documentación sobre la configuración, mantenimiento y operación de la redes de área local.
D-021	Copia de los procedimientos de respaldo y recuperación de datos, descripción de lugares alternos en caso de que exista, periodicidad, lineamiento de etiquetado, entre otros.
D-022	Copia de las pólizas de seguros de equipo electrónico.
D-023	Plan de continuidad y contingencia.
D-024	Detalle de los dispositivos de seguridad para la entrada y salida de datos (firewalls, filtros, entre otros), si se tienen, así como mantenimiento a los mismos.
D-025	Pruebas realizadas a los sistemas de comunicación, que validen la seguridad de entrada y salida de los datos.
D-026	Copia del plan de capacitación a usuarios, así como plan de capacitación interna en el Departamento de Tecnología de Información.
D-027	Copia si existe de la evaluación del cumplimiento del plan anual operativo.
D-028	Copia de los reportes de monitoreo realizado por el DBA, (tunning, valoración de índices, entre otros.
D-029	Definición de los periodos de retención de información de la entidad.

D. Matriz de Calificación de la Gestión de TI

Objetivo: Determinar el grado de cumplimiento de los objetivos de control y nivel de madurez para cada proceso evaluado del marco para la gestión de TI de la entidad.
Instrucciones generales:

i. El cuestionario debe ser llenado por el auditor.

ii. El cuestionario se dispondrá en el sitio WEB de la Superintendencia, el documento estará dividido en los procesos que el estándar **Cobit®** define para cada dominio de TI.

iii. Para cada proceso se establece un conjunto de preguntas sobre los objetivos de control detallados como de los niveles de madurez. Las preguntas que se plantean son de respuesta cerrada Sí, No y **No Ap**lica (NA) y para cada una se debe incluir la referencia a

la documentación utilizada como evidencia. La referencia debe indicar el código dispuesto según la sección II anterior, en caso de otro tipo de referencia deberá indicar el legajo, la sección y el número de página de los papeles de trabajo donde se puede encontrar la documentación de evidencia.

iv. A continuación se ejemplifica la forma en que se debe llenar el cuestionario:

Áreas de Revisión **PO9 Valorar y Administrar los Riesgos de TI**		**Evaluación**				Referencias
		Sí	**No**	**NA**		
PO9.3	Valoración del Riesgo					
	La valoración de la probabilidad de ocurrencia y el impacto de los riesgos identificados se lleva a cabo:					
	1. Sobre una base recurrente.		**1**			
	2. Utilizando métodos cualitativos.	**1**				
	3. Utilizando métodos cuantitativos.			**1**		
	¿Existen las políticas y procedimientos para asegurar la determinación del impacto y la probabilidad de ocurrencia del riesgo inherente?	**1**				
	¿Existen las políticas y procedimientos para asegurar la determinación del impacto y la probabilidad de ocurrencia del riesgo residual?		**1**			

En el ejemplo se observan tres preguntas principales. La primera es compuesta y se subdivide en tres, en este caso se deberán contestar las sub preguntas numeradas (para el ejemplo: 1 ,2 y 3), dejando en blanco la sección de evaluación de la pregunta principal. Las siguientes dos preguntas no son compuestas y se deben responder directamente en la sección de evaluación y en la línea que se encuentran.
Nótese que la sección de evaluación está compuesta por tres columnas para cada respuesta posible: Sí, No y NA (No Aplica), para cada respuesta se debe indicar solo una respuesta y se debe hacer colocando un número 1 en la celda correspondiente.
Por último, en la sección de Referencias se deben indicar las referencias a la documentación utilizada como evidencia, esto se debe hacer utilizando el formato indicado con anterioridad. La sección de observaciones debe ser utilizada por el auditor de TI para explicar las razones por las cuales brinda una respuesta afirmativa o negativa o porque una pregunta en particular no aplica. Pueden brindarse estadísticas para un mejorar comprensión de la respuesta brindada

C. PLAN CORRECTIVO Y/O PREVENTIVO

Nombre de la entidad:
Elaborado por:
Aprobado: <indicar la sesión de Junta Directiva o autoridad equivalente>
Fecha: <*dd/mm/aaaa*>

Resumen Ejecutivo

<Escriba un resumen del plan, contiene una explicación de alto nivel de los objetivos, alcance, supuestos, proyectos, costos y estimación de tiempo para ejecución>

Plan Detallado

Acciones correctivas

<Enumere las acciones que planean ejecutar para atender los hallazgos apuntados en el informe de SUGEF>

Acción/Actividad	Fecha inicio	Fecha finalización	Responsable	Recurso interno / externo	# de hallazgo
Acción 1					
Actividad 1.1					
Actividad 1.2					
Acción 2					

Acciones preventivas

<Enumere las acciones que planean ejecutar para atender los hallazgos apuntados en el informe de SUGEF>

Acción/Actividad	Fecha inicio	Fecha finalización	Responsable	Recurso interno / externo	# de hallazgo
Acción 1					
Actividad 1.1					
Actividad 1.2					
Acción 2					

Lista de Involucrados

El plan tiene el siguiente inventario de involucrados:

Nombre	Dependencia	Número(s) de teléfono	Correo Electrónico

Anexos

<Anexe los documentos o información que considere necesaria para obtener un conocimiento detallado de las acciones a ejecutar>

Nota:

Recurso interno / externo: Se refiere a si las acciones se atienden con personal de TI de la entidad o si requiere de la participación de terceros –expertos para su realización.