SUGEF 14-09

REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 6, del acta de la sesión 773-2009. Celebrada el 20 de febrero del 2009. Publicado en el diario oficial La Gaceta N°50 del jueves 12 de marzo del 2009.

Rige a partir de su publicación en la Gaceta

Versión documento	Fecha de actualización
10	29 de octubre 2012

CONSIDERANDOS

1. El aumento de la dependencia tecnológica que caracteriza el desarrollo de las actividades financieras, la escala y los costos de las inversiones actuales y futuras en sistemas de información, la proliferación de amenazas y eventos no deseados; y el potencial que poseen las tecnologías para cambiar drásticamente los procesos de negocio de las organizaciones, hacen necesario que la gestión del riesgo tecnológico se realice de acuerdo con las mejores prácticas en la materia.

2. La administración del riesgo tecnológico requiere de las entidades financieras la implementación de un marco robusto de gestión y control. El marco Cobit® de amplia aceptación mundial, representa el consenso de los expertos de las buenas prácticas para la gestión y el control de la Tecnología de Información, a través de un lenguaje común comprensible para todos los interesados. Como marco genérico facilita la inclusión de otros estándares para el tratamiento específico de temas relacionados con tecnología, dejando un margen para la libre elección según las necesidades de cada entidad.

3. El marco Cobit® permite atender las recomendaciones emitidas por el Comité de Basilea, particularmente las disposiciones de Basilea II sobre gestión de los riesgos operativos en su dimensión tecnológica, constituyendo asimismo una base de referencia para la evaluación de la gestión de TI de las entidades financieras.

4. La aplicación de la Normativa de Tecnología de Información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras aprobada por el Consejo Nacional de Supervisión del Sistema Financiero mediante artículo 10 del acta de la sesión 347-2002, del 19 de diciembre del 2002, ha evidenciado que existe una base de conocimiento y experiencia en el sistema financiero en relación con el tema tecnológico, sus procesos y riesgos que facilitan la transición al nuevo enfoque reglamentario.

5. Conforme el artículo 171 de la Ley Reguladora del Mercado Valores, es potestad del Consejo Nacional de Supervisión del Sistema Financiero aprobar las disposiciones referentes a la periodicidad, el alcance, los procedimientos y la publicación de los informes rendidos por las auditorías externas de las entidades fiscalizadas.

6. El artículo 131, incisos c) y n) literal ii) de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558, establece como función del Superintendente General de Entidades Financieras proponer al Consejo, para su aprobación, las normas que estime necesarias para el desarrollo de las labores de fiscalización y vigilancia, referentes a periodicidad, alcance, procedimientos y publicación de los informes de las auditorías externas de las entidades fiscalizadas, con el fin de lograr la mayor confiabilidad de estas auditorías. La Superintendencia podrá revisar los documentos que respalden las labores de las auditorías externas, incluso los documentos de trabajo y fijar los requisitos por incluir en los dictámenes o las opiniones de los auditores externos.

7. El artículo 69 de la Ley Orgánica del Banco Central de Costa Rica somete al Sistema Nacional de Pagos Electrónicos (*SINPE*) a la vigilancia y fiscalización de la Superintendencia General de Entidades Financieras.

8. La Superintendencia General de Entidades Financieras tiene la responsabilidad de velar por la estabilidad y eficiencia de sus entidades fiscalizadas mediante el establecimiento de disposiciones y procesos de supervisión que tiendan a minimizar los niveles de riesgo que puedan presentar en el área de tecnología de información.

resolvió, en firme:

aprobar el Acuerdo SUGEF 14-09, "*Reglamento sobre la Gestión de la Tecnología de Información*", de conformidad con el texto se adjunta.

ACUERDO SUGEF 14-09

REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

CAPITULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto
Este reglamento tiene por objeto la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI).

Artículo 2. Alcance [3]
Las disposiciones establecidas en este reglamento son aplicables a las entidades supervisadas por la Superintendencia General de Entidades Financieras (en adelante la "*SUGEF*").

Artículo 3. Definiciones [3]
Para los propósitos de este reglamento se entiende como:

a) ***Autenticación:*** Conjunto de técnicas y procedimientos utilizados para verificar la identidad y autorización de clientes.
b) ***Autoridad equivalente****:* Órgano directivo equivalente a la Junta Directiva en sus funciones, según la naturaleza jurídica de la entidad; por ejemplo: Consejo de Administración para las cooperativas de ahorro y crédito y Directorio para las asociaciones mutualistas.
c) ***Banca electrónica:*** Servicios financieros suministrados a través de medios electrónicos. Comprende un conjunto de canales de comunicación compuestos por hardware y software, mediante los cuales, las personadas físicas o jurídicas pueden acceder vía remota a una entidad financiera para obtener información o realizar operaciones financieras.
d) ***Cobit®:*** Marco de referencia de buenas prácticas para el control de TI. Acrónimo en inglés de Objetivos de Control para la Información y la Tecnología Relacionada, emitido por el IT Governance Institute®.
e) ***Director:*** Cualquier persona física integrante de una junta directiva, de un consejo de administración o de cualquier otro órgano directivo equivalente en sus funciones a los dos primeros.
f) ***Dominio:*** Cada una de las áreas lógicas del ciclo de gestión de TI, utilizadas por Cobit® para agrupar los procesos y objetivos de control. Los cuatro dominios son: Planear y Organizar (*PO*), Adquirir e Implementar (*AI*), Entregar y Dar Soporte (*DS*), y Monitorear y Evaluar (*ME*).
g) ***Auditor de TI:*** Miembro de una firma o despacho o profesional independiente, calificado para ejecutar auditorías en materia de TI conforme los requisitos dispuestos en este reglamento.
h) ***Gestión de la tecnología de información:*** Estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la tecnología de información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.
i) ***Hallazgo:*** Se refiere a las debilidades, deficiencias o brechas apreciables respecto a un criterio o estándar previamente definido.
j) ***Nivel de madurez:*** Cada uno de los grados de desarrollo alcanzado en cada uno de los procesos Cobit®. Los cinco niveles de madurez son:

1. ***Inicial:*** Los procesos son ad-hoc y desorganizados.
2. ***Repetible:*** Los procesos siguen un patrón regular.
3. ***Definido:*** Los procesos se documentan y se comunican.
4. ***Administrado:*** Los procesos se monitorean y se miden.
5. ***Optimizado:*** Las mejores prácticas se siguen y se automatizan.

k) ***Perfil tecnológico:*** Descripción de la estructura organizacional, los procesos y la infraestructura de TI de la entidad, así como del nivel de automatización de sus procesos de negocio y de gestión del riesgo.

l) ***Proceso:*** Cadena de actividades que agregan valor y permiten la generación de un producto o servicio bajo determinadas condiciones y plazo.

m) ***Proveedor de tecnologías de información****:* Persona física o jurídica que provee o presta un servicio relacionado con la tecnología de información, sea independiente o que pertenezca al mismo grupo o conglomerado financiero, incluyendo las casas matrices.

n) ***Riesgo de TI:*** Posibilidad de pérdidas financieras derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la entidad, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información.

o) ***Tecnología de información (TI):*** Conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

p) ***Trabajo para atestiguar:*** Labor ejecutada por un auditor que tiene por objeto expresar una conclusión sobre el resultado de la auditoría de los procesos del marco para la gestión de TI.

Artículo 4. Lineamientos Generales [3]

El Superintendente emitirá, mediante resolución razonada, los contenidos del Perfil Tecnológico de las entidades, las condiciones para la ejecución e informe de la auditoría externa y el formato del Plan Correctivo-Preventivo dispuestos en este reglamento.

CAPITULO II
GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Artículo 5. Objetivos de la Gestión de TI

La gestión de la tecnología de información, debe orientarse al cumplimiento de los siguientes objetivos:

a) ***Alineación Estratégica:*** La TI es congruente con las estrategias y objetivos de la entidad.

b) ***Administración del Riesgo de TI:*** Los riesgos relacionados con TI son conocidos y administrados.

c) ***Entrega de Valor:*** La TI contribuye en la consecución de los beneficios esperados, eficiencia, productividad y competitividad de la entidad.

d) ***Gestión de Recursos:*** La inversión en TI se ajusta a las necesidades de la entidad y es administrada adecuadamente.

e) ***Medición del Desempeño de TI:*** El desempeño de TI es medido y sus resultados son utilizados para la toma de decisiones.

Artículo 6. Marco para la Gestión de TI [3]
La entidad debe diseñar, implementar y mantener un marco para la gestión de la tecnología de información.

El marco para la gestión de TI debe ser congruente con el perfil tecnológico de la entidad, la naturaleza y la complejidad de sus operaciones y contar con la aprobación de la Junta Directiva o autoridad equivalente.

Sin detrimento de lo anterior, el marco para la gestión de TI debe incluir al menos los procesos identificados como obligatorios en el anexo 1 de este reglamento.

La entidad que contrate parte o la totalidad de sus procesos a proveedores locales o extranjeros de tecnologías de información deben incluir obligatoriamente el proceso DS2 "*Administrar los servicios de terceros*" dentro de su marco para la gestión de TI.
En el anexo 1 se muestra la categorización de los 34 procesos que integran la versión de Cobit® y su clasificación para efectos de este artículo.

Artículo 7. Comité de TI y funciones [3]
Cada entidad debe designar un Comité de Tecnología de Información (Comité de TI), el cual debe contar con un reglamento interno de funcionamiento formalmente aprobado por su Junta Directiva o autoridad equivalente. Dicho comité de TI es una instancia asesora y de coordinación en temas de tecnología y su gestión.

El comité responde a la Junta Directiva o autoridad equivalente y le corresponde entre otras funciones, las siguientes:

a) Asesorar en la formulación del plan estratégico de TI.
b) Proponer las políticas generales sobre TI.
c) Revisar periódicamente el marco para la gestión de TI.
d) Proponer los niveles de tolerancia al riesgo de TI en congruencia con el perfil tecnológico de la entidad.
e) Presentar al menos semestralmente o cuando las circunstancias así lo ameriten, un reporte sobre el impacto de los riesgos asociados a TI.
f) Monitorear que la alta gerencia tome medidas para gestionar el riesgo de TI en forma consistente con las estrategias y políticas y que cuenta con los recursos necesarios para esos efectos.
g) Recomendar las prioridades para las inversiones en TI.
h) Proponer el Plan Correctivo-Preventivo derivado de la auditoría y supervisión externa de la gestión de TI.
i) Dar seguimiento a las acciones contenidas en el Plan Correctivo-Preventivo.

Artículo 8. Integración y operación del Comité de TI [4]
El Comité de TI estará integrado al menos por:

a) Un director propietario.
b) El gerente general de la entidad.
c) El responsable del área informática.
d) El responsable de la función de Riesgos.

El Comité será presidido, de forma permanente, por alguno de sus miembros. Cada miembro tiene derecho a voz y voto y serán responsables de cumplir a cabalidad las funciones encomendadas por este reglamento y las definidas por la Junta Directiva o autoridad equivalente.

El Comité de TI podrá contar con la participación de los responsables de las áreas de negocio de la entidad y con asesores externos a la organización cuando lo considere necesario.

El Comité de TI deberá reunirse con la periodicidad que estime pertinente para el cumplimiento de sus fines y todas las sesiones y acuerdos deberán hacerse constar en actas debidamente detalladas, suscritas por los miembros asistentes.

Los grupos y conglomerados financieros pueden constituir un Comité de Tecnología de Información (Comité de TI) corporativo, con un mínimo de cuatro miembros. La conformación la determinará el propio grupo o conglomerado financiero; el mínimo de cuatro miembros debe ser conformado como sigue: una persona de la alta administración, un miembro de junta directiva u órgano equivalente, una persona de los responsables de las áreas de Informática y una persona de los responsables de las áreas de Riesgos, todos los miembros anteriores, provendrán necesariamente de las empresas del Grupo o Conglomerado financiero.

El Comité de TI corporativo y el Comité de TI individual, pueden ser uno solo, siempre que el Comité de TI corporativo, realice las mismas funciones y responsabilidades que se estipulan en esta normativa para el Comité de TI individual, y cumpla las demás funciones y requerimientos, de las normativas especiales que le sean aplicables a cada una de las entidades que conforman el grupo o conglomerado.

En el caso que se determine que el Comité de TI corporativo, no atiende en forma adecuada y oportuna, las funciones y obligaciones indicadas en esta Normativa, para alguna de las entidades que constituyen el grupo o conglomerado, la Superintendencia responsable de la supervisión de dicha entidad, puede requerir que se proceda con la conformación de un comité individual para la respectiva entidad.

En las sesiones del Comité de TI corporativo, cuando se conozcan temas específicos de una de las entidades fiscalizadas, integrantes del grupo o conglomerado, deben encontrarse presentes su Gerente General o el ejecutivo de alto nivel que lo sustituye en su ausencia y el responsable de la Unidad de Informática de dicha entidad, o quien lo sustituya en su cargo, para que las mismas sean válidas.

En las actas de Comité de TI corporativo, se deben separar las deliberaciones y acuerdos, para cada una de las entidades analizadas, cuyos asuntos sean conocidos en la sesión de que se trate. En caso de que en una sesión no se analicen temas de alguna de las entidades que conforma el grupo o conglomerado, se debe dejar constancia de dicha situación en el acta correspondiente.

El libro de actas debe estar a disposición de la Superintendencia correspondiente y de las autoridades judiciales competentes. Las Superintendencias podrán establecer la utilización obligatoria de un libro de actas electrónico, de conformidad con los requisitos que para ese efecto determine el Superintendente correspondiente.

En el caso de entidades financieras supervisadas por la SUGEF, previa solicitud de la entidad interesada, la SUGEF podrá autorizar una conformación distinta a la dispuesta en este artículo, considerando entre otros aspectos la naturaleza jurídica de la entidad, su perfil de negocio, su tamaño

y volumen de actividad, así como la complejidad de sus operaciones.

CAPITULO III
EVALUACIÓN DE LA GESTIÓN DE TI

Artículo 9. Marco Referencial
La evaluación de la Gestión de TI se basará en el marco conceptual de la versión 4.0 de Cobit®, considerando sus cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y Monitorear y Evaluar.

Artículo 10. Perfil Tecnológico
La entidad debe completar el formulario de perfil tecnológico y remitirlo a la SUGEF en la forma y medio que le sea requerido por ésta, en los primeros diez días hábiles del mes de junio de cada año.

El incumplimiento de la remisión del perfil tecnológico, dentro del plazo establecido, será considerado como una negativa a proporcionar información a la Superintendencia, y será sancionado según el artículo 155 inciso a) aparte iii), de la ley Orgánica del Banco Central de Costa Rica .

Artículo 11 Revisión externa independiente
La entidad deberá someterse a una auditoría externa de los procesos que integran el marco para la gestión de TI por parte de un auditor, cuando menos cada dos años.

La SUGEF comunicará a la entidad la fecha de remisión de los productos de la auditoría con una anticipación de por lo menos 9 meses.

Artículo 12. Alcance de la auditoría externa de TI [3]
La auditoría externa de TI abarca los procesos contemplados en el marco para la gestión de TI dispuesto conforme el artículo 6 de este reglamento, indiferentemente de que dichos procesos sean provistos, en parte o totalmente, por la función o área de TI de la entidad o por un proveedor externo.

Artículo 13. Directrices respecto a la auditoría externa de TI [3]
La ejecución de la auditoría externa de TI se rige por las guías y criterios profesionales establecidos para auditoría, aseguramiento y prácticas de control profesional, emitidos por la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association, ISACA, por sus siglas en inglés).

Sin detrimento de lo anterior, el Superintendente podrá establecer condiciones complementarias para la ejecución e informe de la auditoría externa de TI de conformidad con el artículo 4 de este reglamento.

La Superintendencia puede revisar los papeles de trabajo que respalden las labores de auditoría de conformidad con el Artículo 131, literal n inciso ii) de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558.

El representante legal de la entidad supervisada deberá rendir una declaración jurada, donde manifieste que verificó el cumplimiento de los requisitos establecidos para el auditor de TI en el artículo 19 de este reglamento. Dicha declaración deberá mantenerse a disposición de la SUGEF,

quien podrá comprobar el cumplimiento de los requisitos por parte del auditor, cuando lo estime pertinente.

Artículo 14. Comunicado sobre la Gestión de TI y Plan Correctivo-Preventivo
La SUGEF remitirá a la entidad un informe con los principales hallazgos y la calificación sobre la gestión de TI, en el plazo de veinte días hábiles, posteriores a la recepción de los productos de la auditoría externa.

Cuando corresponda, la SUGEF requerirá a la entidad un Plan Correctivo-Preventivo, el cual deberá presentarse a la SUGEF, en un plazo máximo de veinte días hábiles, contados a partir del día siguiente al recibo del comunicado; dicho plazo podrá prorrogarse, previa solicitud de la entidad, hasta por la mitad del plazo dispuesto.

El formato para la presentación del Plan Correctivo-Preventivo se establece por el Superintendente conforme artículo 4 de este reglamento.

Artículo 15. Calificación sobre la Gestión de TI
La SUGEF emitirá una calificación sobre la gestión de TI para cada entidad, calculada a partir de los resultados de la auditoría externa.

La calificación sobre la gestión de TI corresponderá a uno de los siguientes niveles:

Calificación	Nivel
Mayor o igual que 85%	Normal
Mayor o igual que 70% y menor que 85%	Irregularidad 1
Mayor o igual que 55% y menor que 70%	Irregularidad 2
Menor que 55%	Irregularidad 3

Dicha calificación será considerada para juzgar la situación económica-financiera de la entidad conforme el reglamento respectivo.

La calificación sobre la gestión de TI se mantendrá hasta que la SUGEF determine una nueva calificación.

La calificación sobre la gestión de TI considera la ponderación de los siguientes factores:

1. El cumplimiento de los Objetivos de control detallados para cada proceso evaluado.
2. El nivel de madurez alcanzado en cada proceso evaluado.
3. El peso relativo de cada proceso evaluado. El peso asignado lo determina la SUGEF, considerando la importancia relativa del proceso, en virtud del dominio al que pertenece y de su eventual impacto en los procesos de negocio.

El anexo 2 describe el procedimiento para obtener la calificación sobre la gestión de TI.

Artículo 16. Revisión de la calificación
La entidad podrá solicitar, a través de sus representantes legales, una vez concluido el Plan Correctivo –Preventivo requerido conforme el artículo 14, que se modifique su calificación sobre la gestión de TI.

Para su admisión, la solicitud debe cumplir los siguientes requisitos:

a) Carta firmada por el representante legal de la entidad, en la cual se indique los procesos sobre los cuales se solicita una recalificación.
b) Certificación emitida por un auditor de TI, en la cual se indique, para cada uno de los procesos contemplados en el Plan Correctivo –Preventivo, el estado de cumplimiento de los objetivos de control y el nivel de madurez alcanzado.
c) Declaración de la gerencia general, en la que se indique que el resto de los procesos del marco para la gestión de TI, no considerados en el Plan Correctivo- preventivo, no desmejoraron su condición original.

La SUGEF contará con un plazo de veinte días hábiles, contados a partir del día hábil posterior a la recepción de la solicitud, para comunicar a la entidad la nueva calificación.

La SUGEF podrá efectuar por si misma o a través de terceros las verificaciones que estima pertinentes con el propósito de determinar la nueva calificación.

Artículo 17. Recursos
Contra el comunicado sobre la gestión de TI pueden interponerse los recursos ordinarios de revocatoria y/o apelación según lo dispuesto en la Ley General de la Administración Pública, dentro del plazo de ocho días hábiles contados a partir de la notificación del acto.

Artículo 18. Seguimiento y monitoreo por SUGEF
La SUGEF efectuará un seguimiento y monitoreo de la ejecución del Plan Correctivo-Preventivo suministrado por la entidad. Con el objeto de verificar el cumplimiento de las acciones la SUGEF podrá solicitar informes parciales y realizar verificaciones in situ.

Las verificaciones en materia de TI se incluirán dentro de las labores ordinarias de supervisión. En casos extraordinarios la SUGEF podrá efectuar revisiones independientes previo cumplimiento de las formalidades previstas para tal efecto.

Los informes que requiera la SUGEF deberán ser firmados por el responsable del área de TI y el gerente general de la entidad.

Artículo 19. Requisitos del auditor de TI [3]
El auditor de TI que lleve a cabo la ejecución de la auditoría externa de los procesos que integran el marco para la gestión de TI debe cumplir con los siguientes requisitos:

a) Certificado CISA vigente (Auditor Certificado de Sistemas de Información por sus siglas en inglés “Certified Information Systems Auditor”).

b) No haber prestado a la entidad en forma directa o a través de una compañía relacionada, servicios de consultoría, capacitación, o complementarios relacionados con el diagnóstico, implementación y mantenimiento de marcos de control sobre tecnologías de información, durante los últimos tres años anteriores, contados desde la comunicación dispuesta en el artículo 11 de este reglamento.

c) No tener participación relevante en el capital social de la entidad auditada o su grupo o

conglomerado financiero, para tal efecto se adopta la definición de participación relevante dispuesta en el artículo 3 del Acuerdo SUGEF 8-08 Reglamento sobre Autorizaciones de Entidades Supervisadas por la SUGEF, y Sobre Autorizaciones y Funcionamiento de Grupos y Conglomerados Financieros.

d) No tener operaciones en condiciones que signifiquen un trato preferencial respecto a las establecidas para cualquier cliente similar de la entidad auditada, asimismo que no esté clasificado en una categoría de riesgo que ponga en cuestionamiento la recuperación del crédito.

e) No haber desempeñado cargos en la entidad auditada, sus filiales, asociadas, entidades con cometido especial, subsidiarias o su grupo económico durante los dos años anteriores a la fecha de la remisión de los productos de la auditoría.

f) No haber sido declarado insolvente durante los últimos cinco años anteriores a la fecha de la remisión de los productos de la auditoría.

CAPITULO IV
DISPOSICIONES ESPECIALES

Artículo 20. Estándar de seguridad

Sin menoscabo de los objetivos de control de los procesos aplicables de Cobit®, la entidad debe velar que el estándar en materia de seguridad, permita implementar métodos de autenticación para el acceso lógico a los sistemas y servicios informáticos, consecuentes con la criticidad y el valor de los datos y servicios a proteger, debiendo considerar en particular la mejores prácticas en relación con la banca electrónica y otros servicios financieros por internet.

Artículo 21. Tercerización de TI [3]

La entidad que contrate parte o la totalidad de uno o varios procesos o servicios de TI, relacionados con el procesamiento y almacenamiento de datos, independientemente del lugar en donde se lleven a cabo esas actividades, debe mantener las bases de datos actualizadas y las aplicaciones vigentes físicamente en el territorio nacional, accesibles por la SUGEF sin ningún tipo de restricción o condición.

La entidad supervisada es responsable de suministrar la información que le sea requerida por la SUGEF y proveer las facilidades para la ejecución de actividades de supervisión, indistintamente de que los procesos o servicios sean provistos por ella misma, otra empresa del grupo o conglomerado financiero o por un proveedor externo, o que sean llevados a cabo dentro o fuera del territorio costarricense.

DISPOSICIONES FINALES

Artículo 22. Derogatorias

Este Reglamento deroga La "*Normativa de Tecnología de Información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras*" aprobada por el Consejo Nacional de

Supervisión del Sistema Financiero mediante artículo 10 del acta de la sesión 347-2002, celebrada el 19 de diciembre del 2002.

Transitorio I [3]

Para efectos de la aplicación de lo dispuesto en los artículos 6, 11 y 12 de este reglamento, se establece la siguiente gradualidad en los niveles de madurez para los procesos dispuestos como obligatorios en el marco para la gestión de TI y su evaluación externa independiente:

Procesos COBIT®	Primera Auditoría Externa	Segunda Auditoría Externa	Auditorías subsecuentes
PO9 Evaluar y administrar los riesgos de TI	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
PO10 Administrar proyectos			
AI6 Administrar cambios			
DS2 Administrar los servicios de terceros			
DS4 Garantizar la continuidad del servicio			
DS5 Garantizar la seguridad de los sistemas			
DS11 Administrar los datos			
ME2 Monitorear y evaluar el control interno			
PO1 Definir un plan estratégico de TI	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
PO3 Determinar la dirección tecnológica			
PO5 Administrar la inversión en TI			
AI3 Adquirir y mantener infraestructura tecnológica			
AI5 Adquirir recursos de TI			
DS3 Administrar el desempeño y la capacidad			
DS 9 Administrar la configuración			
DS10 Administrar los problemas			
DS12 Administrar el ambiente físico			
Resto de los procesos que integran el marco para la gestión de TI	Nivel madurez mínimo requerido: **uno**	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**

La primera auditoría externa podrá ser requerida por la SUGEF luego de transcurrido un año, contado a partir de la entrada en vigencia de este reglamento.

Transitorio II [2]

El envío por primera vez del perfil tecnológico dispuesto en el artículo 10 será, a más tardar, el 30 de octubre del 2009.

Transitorio III [3]

La SUGEF calificará la gestión de TI conforme lo establecido en el artículo 15, a partir de los resultados de la segunda auditoría externa.

Hasta tanto no se cuente con los resultados de esta segunda auditoría externa, para los efectos de la calificación global de la entidad según los Acuerdos SUGEF 24-00 y SUGEF 27-00 se usará la última calificación disponible sobre la gestión de TI determinada por SUGEF, de conformidad con la "Normativa de Tecnología de Información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras" aprobada por el Consejo Nacional de Supervisión del Sistema Financiero mediante artículo 10 del acta de la sesión 347-2002, celebrada el 19 de diciembre del 2002.

Transitorio IV

Para efectos de lo dispuesto en el artículo 15 los ponderadores de los procesos de la primera evaluación son los siguientes:

Dominio	Procesos COBIT® 4.0	Peso
PO	*PO1 Definir un plan estratégico de TI*	Tres
	PO3 Determinar la dirección tecnológica	
	PO5 Administrar la inversión en TI	
	PO9 Evaluar y administrar los riesgos de TI	
	PO10 Administrar proyectos	
AI	*AI3 Adquirir y mantener infraestructura tecnológica*	
	AI5 Adquirir recursos de TI	
	AI6 Administrar cambios	
DS	*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	
	DS9 Administrar la configuración	
	DS10 Administrar los problemas	
	DS11 Administrar los datos	
	DS12 Administrar el ambiente físico	
ME	*ME2 Monitorear y evaluar el control interno*	
PO	PO2 Definir la arquitectura de la Información	Dos
	PO4 Definir los procesos, organización y relaciones de TI	
	PO6 Comunicar las aspiraciones y la dirección de la gerencia	
	PO7 Administrar recursos humanos de TI	
	PO8 Administrar la calidad	
AI	AI1 Identificar soluciones automatizadas	
	AI2 Adquirir y mantener software aplicativo	
	AI4 Facilitar la operación y el uso	
	AI7 Instalar y acreditar soluciones y cambios	
DS	DS1 Definir y administrar los niveles de servicio	
	DS6 Identificar y asignar costos	
	DS7 Educar y entrenar a los usuarios	
	DS8 Administrar la mesa de servicio y los incidentes	
	DS13 Administrar las operaciones	
ME	ME1 Monitorear y evaluar el desempeño de TI	
	ME3 Garantizar el cumplimiento regulatorio	
	ME4 Proporcionar gobierno de TI	

Rige a partir de su publicación en el diario oficial "La Gaceta". [1]

ANEXO 1
CATEGORIZACIÓN DE PROCESOS Y NIVEL DE MADUREZ REQUERIDO

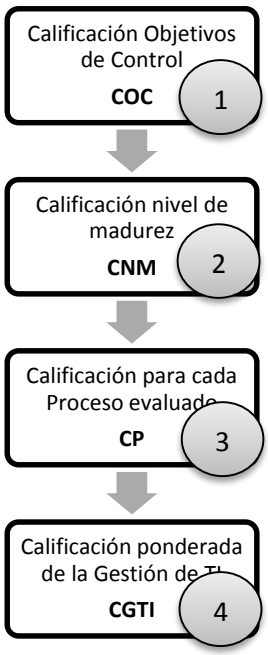
Dominio	Procesos COBIT® 4.0	Marco para la Gestión De TI
PO	PO1 Definir un plan estratégico de TI	Procesos obligatorios Nivel de madurez requerido: Tres
	PO3 Determinar la dirección tecnológica	
	PO5 Administrar la inversión en TI	
	PO9 Evaluar y administrar los riesgos de TI	
	PO10 Administrar proyectos	
AI	AI3 Adquirir y mantener infraestructura tecnológica	
	AI5 Adquirir recursos de TI	
	AI6 Administrar cambios	
DS	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	
	DS9 Administrar la configuración	
	DS10 Administrar los problemas	
	DS11 Administrar los datos	
	DS12 Administrar el ambiente físico	
ME	ME2 Monitorear y evaluar el control interno	
PO	PO2 Definir la arquitectura de la Información	Procesos seleccionables según perfil de TI de la entidad Nivel de madurez requerido: Tres
	PO4 Definir los procesos, organización y relaciones de TI	
	PO6 Comunicar las aspiraciones y la dirección de la gerencia	
	PO7 Administrar recursos humanos de TI	
	PO8 Administrar la calidad	
AI	AI1 Identificar soluciones automatizadas	
	AI2 Adquirir y mantener software aplicativo	
	AI4 Facilitar la operación y el uso	
	AI7 Instalar y acreditar soluciones y cambios	
DS	DS1 Definir y administrar los niveles de servicio	
	DS6 Identificar y asignar costos	
	DS7 Educar y entrenar a los usuarios	
	DS8 Administrar la mesa de servicio y los incidentes	
	DS13 Administrar las operaciones	
ME	ME1 Monitorear y evaluar el desempeño de TI	
	ME3 Garantizar el cumplimiento regulatorio	
	ME4 Proporcionar gobierno de TI	

*La entidad que contrate parte o la totalidad de sus procesos a proveedores locales o extranjeros de tecnologías de información deben incluir obligatoriamente el proceso DS2 “Administrar los servicios de terceros” dentro de su marco para la gestión de TI.

ANEXO 2

PROCEDIMIENTO PARA OBTENER LA CALIFICACIÓN SOBRE LA GESTIÓN DE TI

El procedimiento para obtener la calificación sobre la gestión de TI, consta de cuatro pasos: (1) calificación del cumplimiento de los objetivos de control asociados a cada proceso, (2) Calificación del nivel de madurez alcanzado por cada proceso, (3) determinación de la calificación para cada proceso y (4) Calificación ponderada de la Gestión de TI.



Para los efectos, la metodología se expondrá a lo largo de este anexo mediante un ejemplo.

Planteamiento del ejemplo:

La evaluación de la gestión de TI considera cada uno de los dominios del marco Cobit®; a través del cumplimiento de los objetivos de control y el nivel de madurez, para un número específico de procesos contenidos en el maco para la gestión de TI.

El desarrollo de los cálculos se efectúa únicamente para el proceso denominado "*Proceso A*" del dominio Monitoreo y Evaluación; para los procesos B, C y D se asumen calificaciones que luego se integran en el paso 4 al cálculo de la Calificación ponderada de la Gestión de TI.

Dominio	Proceso	Calificación del proceso supuesta
Planeación y Organización	B	50%
Adquisición e implementación	C	80%
Entrega y soporte	D	65%

A. CALIFICACIÓN DEL PROCESO EVALUADO.

Factor 1: Calificación del cumplimiento de los objetivos de control asociados a cada proceso. (PASO 1)

1. Mediante la "*Matriz de Calificación de la Gestión de TI*" se determina el nivel de cumplimiento de cada objetivo de control asociado a un proceso en particular.
2. La "*Matriz de Calificación de la Gestión de TI*" establece un conjunto de preguntas de respuesta cerrada, asociado a cada objetivo de control; según corresponda se asigna alguna de las siguientes respuestas:

Respuesta	Descripción
SI	La entidad cumple con lo requerido para el objetivo de control evaluado
NO	La entidad no cumple con lo requerido para el objetivo de control evaluado
NA	El objetivo de control no aplica. Este resultado debe observarse como un caso excepcional

Para el ejemplo, la siguiente imagen muestra la forma en que se presenta la calificación para cada objetivo de control que compone el "*Proceso A*".

		Evaluación		
PROCESO A		Si	No	NA
1.1	Objetivo de control detallado A			
1	Pregunta 1	1		
1	Pregunta 2	1		
1	Pregunta 3	1		
		3	0	0
1.2	Objetivo de control detallado B			
1	Pregunta 1	1		
1	Pregunta 2	1		
1	Pregunta 3	1		
		3	0	0
1.3	Objetivo de control detallado C			
1	Pregunta 1	1		
1	Pregunta 2	1		
1	Pregunta 3	1		
1	¿Se asegura que los activos y las inversiones son administrados a través de su ciclo de vida económico?		1	
75%		3	1	0

3. La Calificación de cada Objetivo de Control (*COC*) se obtiene a partir de la siguiente formulación:

***COC*= (Total de respuestas en SI / Total de preguntas aplicables del Objetivo de Control evaluado) * 100**

En nuestro ejemplo, para el objetivo de control 1.3, la calificación es 75%, determinada como (3/4)*100

La calificación total para el factor 1 se obtiene a partir de la siguiente formulación:
∑ COC / (100 * número de objetivos de control evaluados)

Para el ejemplo, 275% / 100 * 3 = 0.9166, donde:

275% = sumatoria de las calificaciones individuales de cada objetivo de control
3 = numero de objetivos de control evaluados

Factor 2: **Nivel de madurez alcanzado en cada proceso (PASO 2)**

1. Mediante la "*Matriz de Calificación de la Gestión de TI*" se determina el nivel de madurez alcanzado en un proceso en particular.
2. La "*Matriz de Calificación de la Gestión de TI*" establece un conjunto de preguntas de respuesta cerrada, asociado a cada proceso. Las preguntas se formulan atendiendo a un nivel de exigencia creciente, de manera que para ascender en la escala, es requisito cumplir con la totalidad de las exigencias del nivel precedente.
3. Las respuestas en la "*Matriz de Calificación de la Gestión de TI*" deben corresponder a alguno de los siguientes estados:

Respuesta	Descripción
SI	La entidad cumple con lo requerido para el nivel de madurez evaluado
NO	La entidad no cumple con lo requerido para el nivel de madurez evaluado
NA	El ítem no aplica. Este resultado debe observarse como un caso excepcional

4. La calificación para cada Nivel de Madurez (*CNM*) se obtiene a partir de la siguiente formulación:
CNM **= Total de respuestas en SI / Total de preguntas del Nivel de madurez evaluado**

5. La asignación del nivel de madurez se inicia en el Nivel 1, para ascender en la escala es requisito indispensable cumplir con la totalidad de las exigencias del nivel inmediato precedente (*CNM = 1*). Se procede a sumar de forma ascendente en la escala los resultados del CNM = 1, deteniéndose en el nivel con un valor CNM diferente a 1.

   Se muestra en la siguiente imagen la forma en que se determina la calificación del nivel de madurez para el "*Proceso A*" del ejemplo.

NIVEL DE MADUREZ		Evaluación Si	No	NA
Nivel 1	Inicial			
1	Pregunta 1	1		
1	Pregunta 2	1		
100%	= 1	2	0	0
Nivel 2	Repetible pero intuitivo			
1	Pregunta 1	1		
1	Pregunta 2	1		
100%	=1	2	0	0
Nivel 3	Proceso definido			
1	Pregunta 1	1		
1	Pregunta 2	1		
1	Pregunta 3		1	
67%	= 0,67	2	1	0
Nivel 4	Administrado y Medible			
1	Pregunta 1	1		
1	Pregunta 2	1		
1	Pregunta 3	1		
100%		3	0	0
Nivel 5	Optimizado			
1	Pregunta 1	1		
1	Pregunta 2	1		
100%		2	0	0
2,67				

6. La calificación obtenida según el procedimiento indicado en el punto anterior para el nivel de madurez, debe ubicarse en el rango de valor que corresponda, según el cuadro siguiente:

Rango	Nivel	Descripción
De 0 a 0.99	0	No existente
De 1 a 1.99	1	Inicial
De 2 a 2.99	2	Repetible
De 3 a 3.99	3	Definido
De 4 a 4.99	4	Administrado
Igual a 5	5	Optimizado

En el ejemplo, una calificación de 2.67 corresponde el Nivel 2 "*Repetible*", para una desviación respecto al nivel de madurez requerido (*Nivel 3*) de -0.33

7. La calificación total para el factor 2 se obtiene a partir de la siguiente formulación:

CNM *100 / (100 * Nivel Requerido)

Para el ejemplo, 2.67*100 / 100 * 3 = 0.89, donde:

2.67 = CNM

3 = Nivel de madurez requerido

Factor 3: **Calificación de cada Proceso evaluado (PASO 3)**

La Calificación de cada Proceso evaluado (*CP*) se establece mediante la suma del producto de cada uno de los factores por su peso, según la siguiente formulación:

CP = Factor 1 * peso factor 1 + Factor 2 * peso factor 2

En donde el peso de los factores es:

Factor	Dimensión	Peso
1	Resultado de la calificación del Objetivos de Control (COC)	70%
2	Resultado de la calificación del Nivel de Madurez (CNM)	30%

Para el ejemplo, corresponden los siguientes resultados:

Factor	Dimensión	Peso	Resultado
1	COC = 0.92	70%	0.6416
2	CNM = 0.89	30%	0.267
		Suma	**0.9086**

La calificación del "*Proceso A*" es **90.86%.**

B. ***CALIFICACIÓN DE LA GESTION DE TI (PASO 4)***

1. Una vez establecida la calificación para cada uno de los procesos incluidos en la evaluación del marco para la gestión de TI, se procede a establecer la Calificación sobre la Gestión de TI (*CGTI*); la cual se obtiene mediante la suma de las calificaciones ponderadas de los procesos evaluados.

   La calificación se obtiene mediante la siguiente formulación:

   CGTI = ∑ (CP ponderada)

   Donde CP ponderada, se obtiene al multiplicar cada CP por el peso asignado al proceso y luego dividirlo entre el total de los pesos.

   Para expresar la calificación final se utilizarán dos dígitos decimales sin redondeo.

   Para el ejemplo, la *CP ponderada* del "*Proceso A*" es 22.71% como resultado de (90.86% * 3) /12.

   La imagen muestra el cálculo y resultado final para el ejemplo:

Descripción	Peso	Resultado	
		CP	*CP ponderada*
Proceso A	**3**	90,83%	**22,71%**
Proceso B	**3**	50,00%	**12,50%**
Proceso C	**3**	80,00%	**20,00%**
Proceso D	**3**	65,00%	**16,25%**
Total	**12**	**CGTI**	**71,46%**

Irregularidad 1

2. El peso asignado (*ponderador*) lo determina la SUGEF, considerando la importancia relativa del proceso en virtud del dominio al que pertenece y de su eventual impacto en los procesos de negocio. La siguiente tabla presenta los valores asignables:

		Impacto a procesos de negocio		
	PESO	Alto	Medio	Bajo
Importancia relativa	Primario	3	3	2
	Secundario	3	2	1
	Residual	2	2	1

LINEAMIENTOS GENERALES
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/GTP/GSC/JLCH/gv1*

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.

MODIFICACIONES

[1] Publicado en el diario oficial la Gaceta N° 50 del jueves 12 de marzo de 2009.

[2] Modificado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 9 del Acta de la Sesión 796-2009, celebrada el 7 de agosto del 2009. Rige a partir de su publicación en el diario oficial. Publicado en el diario oficial "La Gaceta" Nº 160 del 18 de agosto del 2009.

[3] Modificado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 5 del Acta de la Sesión 853-2010, celebrada el 21 de mayo del 2010. Rige a partir de su publicación en el diario oficial "La Gaceta". Publicado en el diario oficial "La Gaceta" Nº 115 del 15 de junio del 2010.

[4] Modificado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 4 del acta de la sesión 1005-2012, celebrada el 9 de octubre del 2012. Rige a partir de su publicación en La Gaceta. Publicado en La Gaceta N° 208 del 29 de octubre del 2012.

HISTORIAL DE CAMBIOS

Versión 01: Texto del reglamento aprobado.

Versión 02: Publicación en La Gaceta N°50 del jueves 12 de marzo del 2009.

Versión 03: Modificación transitorio II del reglamento y publicación formulario de perfil tecnológico.

Versión 04: Modificación de los Lineamientos Generales

Versión 05: Modificación artículos 2, 3, 4, 6, 7, 12, 13, 19, 21 y los transitorios I y III. Rige a partir de su publicación en el diario oficial “La Gaceta”. Pendiente de publicación.

Versión 06: Modificación artículos 2, 3, 4, 6, 7, 12, 13, 19, 21 y los transitorios I y III. Rige a partir de su publicación en el diario oficial “La Gaceta”. Publicado en La Gaceta N° 115, del 15 de junio del 2010.

Versión 07: Modificación de los lineamientos generales.

Versión 08: Actualización de los lineamientos generales 24 enero 2011.

Versión 09: Nuevo formato. Sitio WEB.

Versión 10: Modificación del artículo 8. Rige a partir de su publicación en el Diario Oficial “La Gaceta”. Publicado en La Gaceta N°208 del 29 de octubre del 2012.