22 de marzo del 2017
CNS-1318/09
CNS-1319/11

Señor
Luis Carlos Delgado Murillo, ***Presidente***
CONSEJO NACIONAL DE SUPERVISIÓN
DEL SISTEMA FINANCIERO

Estimado señor:

El Consejo Nacional de Supervisión del Sistema Financiero en los artículos 9 y 11 de las actas de las sesiones 1318-2017 y 1319-2017, celebradas el 13 y el 20 de marzo del 2017 respectivamente,

dispuso, por mayoría y en firme:

I. En cuanto al Reglamento General de Gestión de la Tecnología de Información:

considerando que:

1. Acuerdo SUGEF 14-09: El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), mediante artículo 6, del acta de la sesión 773-2009 del 20 de febrero del 2009 aprobó el Acuerdo SUGEF 14-09 "Reglamento sobre la gestión de la tecnología de información", que define los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras (SUGEF).

2. SUGEF: 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 puede 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.

3. SUGEVAL: El artículo 3 de la Ley Reguladora del Mercado de Valores establece que la Superintendencia General de Valores (SUGEVAL) debe velar por la protección del inversionista y el adecuado funcionamiento del mercado de valores; asimismo el artículo 8 de la Ley 7732, Ley Reguladora del Mercado Valores, inciso b) establece que la SUGEVAL someterá a la consideración del Consejo Nacional los proyectos de reglamento que le corresponda dictar a la Superintendencia, el inciso j) establece la potestad de adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación, supervisión y fiscalización que le competen, y el inciso l) establece la potestad de la Superintendencia para requerir a los supervisados toda la información razonablemente necesaria a fin de cumplir la función supervisora del mercado de valores.

4. SUPEN: El artículo 38, literal f) de la Ley 7523, Régimen Privado de Pensiones, establece como una atribución del Superintendente de Pensiones adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación y fiscalización que le competen a la Superintendencia, según la Ley y las normas emitidas por el Consejo Nacional de Supervisión del Sistema Financiero; por

otra parte el Consejo Nacional de Supervisión del Sistema Financiero, mediante artículo 8, del acta de la sesión 975-2012 del 29 de mayo del 2012 aprobó la evaluación cualitativa del riesgo operativo para el cálculo de la suficiencia patrimonial de las operadoras de pensiones complementarias, donde uno de los componentes es la evaluación de la tecnología de información. Finalmente, mediante artículo 7, del acta de la sesión 1066-2013 del 1 de octubre del 2013 aprobó el Reglamento de Calificación de la Situación Financiera de los Fondos Administrados por los Entes Regulados donde se evalúa el riesgo tecnológico en los regímenes de pensiones de beneficio y contribución definidas.

5. SUGESE: El artículo 29 de la Ley Reguladora del Mercado de Seguros, Ley 8653; establece como objeto de la Superintendencia General de Seguros (SUGESE), velar por la estabilidad y el eficiente funcionamiento del mercado de seguros, así como entregar la más amplia información a los asegurados. La misma ley autoriza a la SUGESE para regular y supervisar a las personas que intervengan en los actos o contratos relacionados con la actividad aseguradora, reaseguradora, la oferta pública y la realización de negocios de seguros. Asimismo, en el inciso i) del citado artículo se establece como su función el proponer al Consejo Nacional, para su aprobación, la normativa reglamentaria que se requiera para la aplicación de esta Ley y para cumplir sus competencias y funciones.

6. CONASSIF: 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.

7. Gestión de TI: La tecnología de la información (TI) es indispensable para gobernar, gestionar y tomar decisiones dentro de las organizaciones, asimismo, su adecuada administración permite mantener la competitividad y coadyuva en la consecución de las metas y objetivos.

   A principios de la década anterior, y en virtud de múltiples casos de quiebras y fraudes asociados a temas operativos y de mala gestión, varios organismos internacionales han emitido disposiciones en las que resaltan la necesidad de mejorar los sistemas de Gobierno Corporativo y en consecuencia, la forma de gobernar TI.

   Estos requerimientos plantean el reto de diseñar y mantener controles eficientes que faciliten la gestión de TI desde dos puntos de vista: el primero, tomando a TI como un proceso más del negocio y segundo, tomando a TI como encargado de proveer y mantener la plataforma y los sistemas que apoyan la ejecución del resto de los procesos del negocio.

   Esta dualidad implica para las entidades el diseño o la adopción de un marco que les permita gobernar, gestionar y controlar la función de TI, desde ambos puntos de vista en forma consistente.

   Dado que la gobernanza orienta, dirige y supervisa la gestión de TI y que las tecnologías de información se consideran factores de riesgo operativo, al que están expuestas las entidades, resulta necesario que este reglamento incluya la evaluación los procesos de gobierno y gestión de TI por parte de las Superintendencias.

8. Necesidad de control de TI: Una inadecuada gestión del riesgo operacional en el área de la tecnología de información en las entidades supervisadas puede repercutir negativamente en la continuidad de sus operaciones; impactando por consiguiente sus patrimonios y concomitantemente, afectando a los clientes de las entidades.

   Por lo anterior, resulta indispensable que las entidades supervisadas determinen su marco de gestión, para el control la tecnología de información, que garantice la integridad, seguridad, auditabilidad y disponibilidad de la información y de los servicios ofrecidos.

9. Sobre la implementación del marco de gestión de TI, dispuesto en este reglamento:
El diseño e implementación del marco de gestión de TI requiere por parte de las entidades supervisadas de esfuerzo planificado y progresivo. Con el objeto de facilitar este proceso, su inversión y la definición concomitante de políticas, procesos y estructuras, el modelo de supervisión basada en riesgos le coadyuva, a través de este reglamento, a que la entidad supervisada establezca su marco de gestión de TI en función de sus necesidades según su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica.

   Los lineamientos generales que acompañan el reglamento establecen un periodo de implementación a partir de la entrada en vigencia (gradualidad) que abarca hasta 5 años para entidades supervisadas por la SUGEVAL, SUPEN y SUGESE; asimismo, de 3 años para las entidades supervisadas por la SUGEF, este último plazo en consideración del avance logrado a partir de los requerimientos del Acuerdo SUGEF 14-09 "Reglamento sobre la Gestión de la Tecnología de Información". Estos plazos se estiman razonables para que las entidades puedan efectuar las adecuaciones necesarias para la implementación efectiva de su marco de gestión de TI.

   Por otra parte, de acuerdo con la experiencia de la aplicación del "Reglamento sobre la Gestión de la Tecnología de Información" en SUGEF, se estima prudente mantener el lapso de nueve meses, contados a partir de la notificación del requerimiento de auditoría externa de TI, para la remisión de los entregables de la auditoría externa de TI del marco de gestión de TI, así como sobre cualquier otro criterio que se considere necesario en virtud del perfil de riesgo de la entidad.

   Dicha holgura permite a las entidades desarrollar los aspectos procedimentales necesarios a efecto de la contratación, ejecución y entrega de los resultados de la auditoría externa. Finalmente, el Consejo ha considerado razonable el plazo de veinte días hábiles para la remisión del plan de acción, cuando haya sido requerido por alguna superintendencia. Dicha conclusión se desprende del hecho que una entidad va recibiendo retroalimentación conforme evoluciona la auditoría externa, de manera que una vez finalizada, ya cuenta con suficientes elementos y datos que le permiten perfilar un conjunto de acciones.

10. Supervisión basada en riesgos: La supervisión basada en riesgos se caracteriza por la migración de un modelo basado en reglas hacia un enfoque donde la entidad supervisada es responsable de una gestión integral de los riesgos del negocio. En este enfoque corresponde a la entidad supervisada determinar, dentro de esa gestión de riesgos el marco de gestión de TI que se adapten a su negocio, de manera que le permita identificar y establecer las medidas de mitigación para los riesgos que surgen de TI; por ello, la regulación se enfoca a un marco de gestión de TI con aquellas características prudenciales suficientes para el supervisor, sin que necesariamente se definan, puntualmente, determinados estándares o herramientas de control. En esta misma lógica, el reglamento que se emite encuentra sentido como parte de una estructura normativa transversal al sistema financiero, que no sustituye lo procesos de supervisión sobre riesgo operacional que ya se desarrollan, sino que viene a complementarlos, aportando información que nutre el criterio del supervisor a partir del aporte de especialistas externos.

11. Estándares disponibles como marco de referencia: La industria y los profesionales en TI, han venido desde hace varias décadas desarrollando estándares y marcos que permitan gestionar y controlar las tecnologías. Ante la incertidumbre y costo que significa el desarrollo interno de un marco de gestión de TI, las organizaciones han propendido por adoptar alguno de los marcos o estándares disponibles.

    Marcos de referencia como Cobit e ITIL y estándares como ISO gozan en la actualidad de aceptación general, desde la visión del supervisor; Cobit es un marco apropiado que se ajusta al negocio y facilita que las organizaciones desarrollen un ambiente de control que responda a las necesidades del negocio, además de estandarizar procesos de TI, limitar desviaciones de los objetivos de negocio y particularmente lograr un balance entre los riesgos que introduce la tecnología de información y su aporte de valor al desempeño y rentabilidad. Estos marcos igualmente permiten el desarrollo del enfoque de supervisión basada en riesgos, por las siguientes razones:

Desde la óptica del negocio:

a. Enfoque en Gobierno de TI: El marco se desarrolla dentro del nuevo enfoque de gobernabilidad de TI como parte del buen gobierno corporativo, procurando mayor involucramiento con los procesos clave, definiendo una estructura de relaciones y procesos diseñados y ejecutados por la entidad para dirigir y controlar la tecnología, sus riesgos y vinculación con las estrategias y objetivos de negocio.
b. Satisface los requerimientos de negocio: Integración más clara entre los objetivos del negocio y la TI, mediante objetivos en el modelo de cascada y métricas que los soportan.
c. Logra la armonización: Integración optimizada de otros estándares internacionales.
d. Definiciones y flujos de procesos: Optimización en las descripciones de los procesos, actividades, entradas y salidas.
e. Lenguaje y presentación: Utiliza un lenguaje accesible para todo tipo de usuario, mismo que permite a ejecutivos no versados en conocimientos tecnológicos identificar y comprender los principales aspectos de TI.

Desde la óptica del supervisor:

f. Permite evaluar la integración de los procesos de TI con los procesos y líneas de negocio y el logro de los objetivos de la entidad.
g. Permite identificar el grado de dependencia de las entidades de la tecnología de información en sus operaciones.
h. Permite identificar los perfiles de riesgo en TI de los supervisados, con el propósito de concentrar esfuerzos en entidades con mayor exposición o con mayores debilidades de control.
i. Es un marco integrador (alineado con otros estándares y buenas prácticas que puede usarse en conjunto con ellas), enfocado al negocio, y diseñado para ser utilizado por una amplia gama de usuarios, pero principalmente, como guía integral para alta administración y para los líderes o responsables de los procesos y líneas de negocio.

12. Sobre la estrategia del supervisor: La experiencia con los intermediarios financieros en relación con el proceso de implementación del marco de gestión de TI del Acuerdo SUGEF 14-09 “Reglamento sobre la Gestión de la Tecnología de Información”, develó que varios grupos y conglomerados financieros gestionan la tecnología de información de forma corporativa en las empresas que los integran. Conscientes de esta realidad, el CONASSIF ha concebido la necesidad de integrar en un solo cuerpo normativo los requerimientos de control para la gestión de TI para un grupo o conglomerado. Dicha estrategia tiene como objetivo permitir entre otros aspectos, la estandarización de procesos, la generación de economías de escala y la creación de una cultura proclive a la mejora de la gobernabilidad de la TI.

    El reglamento que se emite también reconoce que entre los supervisados se presentan diferencias en el grado de dependencia de las tecnologías de información y que, como consecuencia, la materialización de los riesgos a esas tecnologías les impacta de manera diferente. Esa condición se refleja al implementar el principio de “proporcionalidad” que rige los esquemas de supervisión basada en riesgo. Dicho principio promueve que las prácticas y demandas de supervisión se definan y apliquen en consonancia con el perfil de riesgo y la importancia sistémica de los supervisados, el enfoque asumido permite que los supervisados agreguen otros estándares o bien que exista una exigencia particular en función de su rol dentro del mercado en que opera. Finalmente, sobre una base de costo beneficio, naturaleza de la entidad y perfil tecnológico; se permite la definición de marcos de gestión de TI diferentes en reconocimiento de estas diferencias.

    La pretensión última de esta estrategia es generar, bajo un esquema de supervisión integrada y coordinada, mejoras en el nivel de la gestión de la tecnología de información y sus riesgos asociados, como herramienta para contribuir al proceso de gestión de riesgos y de preparación ante los retos que impone un ambiente financiero competitivo e innovador.

13. Auditoría externa: La auditoría de los sistemas de tecnología de información es una actividad altamente especializada para la cual existen certificaciones con reconocimiento mundial; se considera conveniente,

que la revisión del marco de gestión de TI y cualquier otro criterio que las Superintendencias consideren necesario en virtud del perfil de riesgo de las entidades supervisadas, sea ejecutada por auditores externos con el fin de contribuir con la eficiencia en el proceso de supervisión. Los resultados de esta auditoría pueden enriquecer la supervisión en torno a los riesgos operacionales y de tecnología de la información que realizan las Superintendencias y se constituye en un elemento adicional dentro de la supervisión basada en riesgos.

14. Registro de Auditores Elegibles: Actualmente se cuenta con un registro de auditores con requisitos en torno a su capacidad e independencia, dicho registro se concentra en auditores financieros, sin embargo;, con el propósito de ir avanzando en la integración en un solo cuerpo reglamentario, que regule los requerimientos de los distintos profesionales que convergen en procesos de revisión y auditoria, se amplía el alcance de este registro para que incluya a los auditores externos de tecnologías de la información.

15. Comité de TI: El Reglamento de Gobierno Corporativo señala dentro de las funciones del Órgano de Dirección, establecer los comités técnicos que considere pertinentes para la buena gestión de la entidad, por lo que la creación del comité de TI estará en función de las necesidades de las entidades supervisadas según su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y su dependencia tecnológica.

16. Coordinación entre superintendencias: Para evitar costos innecesarios a las entidades supervisadas resulta imprescindible coordinar los procesos de supervisión de las diferentes superintendencias cuando una misma unidad de TI presta servicios a entidades supervisadas por distintos órganos supervisores.

17. El inciso i) del artículo 171 de la Ley Reguladora del Mercado de Valores establece como una de las funciones del Consejo Nacional de Supervisión del Sistema Financiero reglamentar el intercambio de información que podrán realizar entre sí las diferentes Superintendencias, para el estricto cumplimiento de sus funciones de supervisión prudencial. La Superintendencia que reciba información en virtud de este inciso, deberá mantener las obligaciones de confidencialidad a que está sujeto el receptor inicial de dicha información.

resolvió:

Aprobar el Reglamento General de Gestión de la Tecnología de Información, de conformidad con el siguiente texto:

REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto
Este Reglamento establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense.

Artículo 2. Alcance
Las disposiciones establecidas en este Reglamento son de aplicación para:

a) Supervisados por SUGEF:
1. Bancos comerciales del Estado;
2. Bancos creados por ley especial;
3. Bancos privados;
4. Empresas financieras no bancarias;
5. Organizaciones cooperativas de ahorro y crédito;

6. Mutuales de ahorro y préstamo y
7. Caja de ahorro y préstamos de la ANDE;
8. Cualquier otro intermediario financiero sujeto a supervisión por SUGEF.

b) Supervisados por SUGEVAL:
1. Puestos de Bolsa y Sociedades Administradoras de Fondos de Inversión;
2. Bolsas de Valores;
3. Sociedades de compensación y liquidación;
4. Proveedores de Precio;
5. Entidades que brindan servicios de custodia;
6. Centrales de Valores;
7. Sistemas de Anotación Electrónica en Cuenta, y
8. Sociedades titularizadoras y fiduciarias.

c) Supervisados por SUGESE:
1. Entidades Aseguradoras y sociedades Reaseguradoras;
2. Sucursales de entidades aseguradoras extranjeras.

d) Supervisados por SUPEN:
1. Operadoras de Pensiones Complementarias.
2. Fondos complementarios creados por leyes especiales o convenciones colectivas.
3. Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social.

Se exceptúan los regímenes administrados por la Dirección Nacional de Pensiones del Ministerio de Trabajo, las entidades reguladas y fondos en proceso de liquidación, los fondos creados por leyes especiales cuya gestión de TI es contratada a una operadora de pensiones, así como los fondos de pensiones cerrados a nuevas afiliaciones.

Artículo 3. Definiciones y abreviaturas
Para efectos de este Reglamento y sus Lineamientos se utilizan las siguientes definiciones y abreviaturas:

a) Auditor externo de TI: profesional independiente o socio de una firma o despacho responsable de la auditoría externa de TI.

b) Auditoría externa de TI: servicio de auditoría directa que implica un compromiso de reporte directo según el estándar definido por ISACA.

c) Cliente: Persona relacionada a las entidades supervisadas denominadas: ahorrantes, inversionistas, afiliados a fondos de inversión o fondos de pensiones, tomadores de seguros, asegurados, beneficiarios de pólizas de seguros, según sea el caso.

d) Entidad supervisada: entidad del sector financiero supervisada por un órgano supervisor costarricense según el alcance definido en el artículo 2.

e) Gestión de TI: 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.

f) Guías de aseguramiento: guía con los pasos de prueba sugeridos para auditar el cumplimiento de los objetivos de control.

g) Gobierno de TI: componente del marco de gobierno corporativo a través del cual, el Órgano de Dirección y la Gerencia de la entidad o vehículo de administración de recursos de terceros, evalúa, controla y dirige el uso actual y futuro de la tecnología de información, para contribuir con el soporte de las metas estratégicas y el monitoreo en el cumplimiento de los planes.

h) Hallazgo: debilidad, deficiencia o brecha apreciable respecto a un criterio o estándar previamente definido.

i) ISACA: acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association).

j) Marco de Gestión de TI: conjunto de procesos, destinados a gestionar las tecnologías de información, que la entidad supervisada debe adoptar como referencia para la gestión integral de sus riesgos tecnológicos, considerando su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica que éstas tienen en procesos de TI.

k) Objetivo de control: declaración del resultado o fin que se desea lograr, al implantar procedimientos de control en una actividad de TI en particular.

l) Órgano de Dirección: Máximo órgano colegiado de la entidad, responsable de la organización.

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

n) Plan de acción: documento que describe las acciones, plazos y responsables que establezca una entidad supervisada, para atender los hallazgos y riesgos detectados y comunicados en el reporte del supervisor.

o) Prácticas de control: indicaciones detalladas para dar cumplimiento a los objetivos de control.

p) Proceso de negocio: cadena de actividades que agregan valor y permiten la generación de un producto o servicio bajo determinadas condiciones y plazo.

q) Proveedor de TI: persona física o jurídica que provee o presta un servicio relacionado con TI a la unidad de TI, o a una entidad supervisada, sea independiente o que pertenezca al mismo grupo o conglomerado financiero, incluyendo las casas matrices, indistintamente de su domicilio.

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

s) TI: acrónimo de Tecnologías de Información, definidas como el conjunto de técnicas para la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos de negocios, 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, entre otros.

t) Tipo de gestión de TI: Conjunto de características o aspectos que determinan si la gestión que realizan las entidades es individual o corporativa.

u) Unidad de TI: unidad que provee los procesos y servicios de TI para las entidades supervisadas.

Artículo 4. Lineamientos Generales
Los superintendentes deben emitir conjuntamente, mediante acuerdo de alcance general, los Lineamientos Generales para la aplicación de este Reglamento.

Artículo 5. Coordinación entre superintendencias
Las superintendencias deben coordinar los procesos regulados en este reglamento cuando la gestión de TI sea corporativa, cuando existan razones técnicas y de oportunidad que justifican dicho accionar.

El proceso de intercambio de información entre superintendencias se hará en los términos dispuestos en la Ley Orgánica del Banco Central de Costa Rica.

CAPITULO II

ORGANIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

Artículo 6. Unidad de TI
La Unidad de TI es individual, cuando ésta forma parte de la estructura organizativa de la entidad supervisada, o es un proveedor de TI domiciliado en el territorio nacional o en el extranjero, que brinda servicios en forma particular a una entidad supervisada.

La Unidad de TI es corporativa, cuando el servicio lo realiza una unidad que forma parte de la estructura organizacional de una empresa integrante del mismo grupo o conglomerado financiero al que pertenece la entidad supervisada, o bien, es un proveedor de TI domiciliado en el territorio nacional o en el extranjero, que brinda servicios a varias empresas integrantes de un mismo grupo o conglomerado financiero.

La responsabilidad del gobierno, la gestión y de la seguridad de información en los servicios que estén tercerizados recaerá en las entidades supervisadas.

Artículo 7. Gobierno de TI
Las entidades supervisadas deben establecer una estructura de gobierno de TI con actividades y propósitos orientados a la generación de valor, a la consecución de beneficios acorde a los niveles de riesgo aceptables y al uso óptimo de los recursos de las tecnologías de la información.

Las entidades supervisadas deben procurar que las necesidades de las partes interesadas sean evaluadas respecto a las metas corporativas establecidas; instituir una dirección del gobierno y de la gestión de TI priorizada; y asegurar que sea monitoreado el rendimiento y el cumplimiento respecto a la dirección y las metas acordadas.

Artículo 8. Gestión de TI
Las entidades supervisadas son responsables de planificar, implementar, controlar y mantener un marco de gestión de TI, conforme a los procesos descritos en los Lineamientos Generales y considerando los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el órgano de dirección de cada una de las entidades.

El marco de gestión de TI debe formularse, considerando las particularidades de cada entidad supervisada, en atención a su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica. Cualquier otra particularidad o aspecto puede ser considerada por la entidad supervisada o por la Superintendencia. Los procesos del marco de gestión de TI que no aplican para su modelo de negocio deberán ser justificados razonadamente mediante un estudio técnico.

Cuando la gestión de TI sea tipificada como corporativa, la entidad puede coordinar, aplicar y mantener un único marco de gestión de TI corporativo, el cual debe contemplar los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el órgano de dirección de cada una de las entidades.

De acuerdo con las necesidades de supervisión, el riesgo identificado, o cuando se determine que el marco de gestión de TI no es acorde a las particularidades de la entidad supervisada, las Superintendencias pueden requerir, mediante resolución razonada, la inclusión de procesos en el marco de gestión de TI establecido por las entidades supervisadas.

CAPITULO III

DE LA SUPERVISIÓN Y AUDITORÍA EXTERNA DE TI

Sección I: Perfil tecnológico y tipo de gestión de TI

Artículo 9. Perfil tecnológico
Cada entidad supervisada debe elaborar y mantener actualizado su perfil tecnológico. El formulario de perfil tecnológico, la fecha de envío a la Superintendencia respectiva, forma y medio serán establecidos en los Lineamientos Generales.

Cuando la unidad de TI es corporativa debe remitirse un único perfil y coordinar que ese perfil tecnológico se ajuste al marco de gestión de TI. El perfil tecnológico debe identificar las particularidades de cada una de las entidades.

Artículo 10. Tipo de gestión de TI
Las entidades supervisadas pueden solicitar que su gestión de TI sea tipificada como corporativa cuando la unidad de TI provee servicios a dos o más entidades integrantes del grupo o conglomerado financiero. Los aspectos a considerar en la justificación de la solicitud y el plazo de resolución serán establecidos en los Lineamientos Generales.

Sección II: Auditoría Externa de TI

Artículo 11. Auditoría de las Tecnologías de Información
El supervisor solicitará a las entidades supervisadas la contratación de una auditoría externa de TI sobre sobre el marco de gestión de TI y su aplicación, lo anterior según se determine en el alcance de la auditoría definido por el supervisor.

El intervalo entre una y otra solicitud no puede ser menor a dos años ni mayor a cuatro años, excepto, cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de adelantarla.

La auditoría externa de TI debe cumplir con el ciclo de auditoría de TI conforme a las Normas de Auditoría y Aseguramiento de Sistemas de Información emitidas por ISACA.

Sin embargo; los superintendentes pueden establecer mediante los Lineamientos Generales criterios complementarios para la ejecución del ciclo de la auditoría.

El auditor externo de TI que lleve a cabo esta auditoría debe estar inscrito en el Registro de Auditores Elegibles que forma parte del Registro Nacional de Valores e Intermediarios, dispuesto en la Ley Reguladora del Mercado de Valores de conformidad con el reglamento correspondiente.

El contrato con el auditor externo de TI debe incluir una cláusula que obligue a éste a entregar al supervisor, copia de la información recopilada y procesada que sirve como respaldo de las labores de auditoría, así como los papeles de trabajo, en un plazo máximo de cinco días hábiles contados a partir de recibida la solicitud de entrega.

Si la unidad de TI es corporativa le corresponde a los Órganos de Dirección asegurarse que el alcance de la auditoría incluya todo aquello que corresponde a cada una de las entidades supervisadas, de tal forma, que los productos a entregar evalúen la gestión de TI a nivel de los procesos, pero también incluya aquellos riesgos particulares del negocio que desarrolla cada entidad supervisada. En caso de que se contrate una auditoría externa corporativa, los Órganos de Dirección de las entidades supervisadas deben dejar constancia de la aprobación del contrato de servicios, el cual debe cumplir con todos los requisitos establecidos en las regulaciones vigentes.

Artículo 12. Alcance y plazo de la auditoría
El supervisor debe comunicar a las entidades supervisadas el alcance y plazo de remisión de los productos entregables de la auditoría externa de TI.

El alcance lo establece el supervisor mediante la definición de al menos los aspectos siguientes:
a) Procesos y objetivos de control a evaluar, con base en el marco de gestión de TI aplicables en el momento de la solicitud de la auditoría externa de TI.
b) Entidades supervisadas y áreas de negocio a considerar en cada proceso.
c) Servicios de TI suministrados por proveedores de TI.
d) El periodo de cobertura.

El plazo otorgado para la remisión de los productos entregables será definido en los Lineamientos Generales.

Artículo 13. Productos entregables
Las entidades supervisadas deben remitir al supervisor los productos siguientes:
a) El informe de auditoría externa de TI, según el formato establecido en los Lineamientos Generales.
b) La matriz de evaluación de los procesos auditados.
c) Copia del acta del Órgano de Dirección de la entidad, en el cual aprueba el informe de la auditoría externa de TI.

Artículo 14. Presentación de resultados de la auditoría externa de TI
Las entidades supervisadas deben convocar, previa coordinación con el supervisor, una reunión de salida para la presentación de los resultados de la auditoría externa de TI.

El plazo otorgado para convocar la presentación de resultados de la auditoría externa será definido en los Lineamientos Generales.

El auditor externo de TI debe presentar los resultados de la auditoría externa de TI. Los contenidos mínimos de la presentación se establecen en los Lineamientos Generales.

En la presentación de resultados de la auditoría externa deben participar al menos las personas siguientes:

a) Los colaboradores que estimen las superintendencias.
b) El Gerente General de las entidades supervisadas.
c) El responsable de la unidad de TI, o similar, de las entidades supervisadas.
d) El auditor interno, cuando exista, de cada una de las entidades supervisadas.
e) El presidente del comité de vigilancia, cuando exista, de cada una de las entidades supervisadas.

Sección III: Reporte supervisor y plan de acción

Artículo 15. Reporte de Supervisión
De los resultados de las auditorías externas de TI de las entidades supervisadas, las superintendencias elaborarán un reporte de supervisión. Este reporte debe elaborarse y actualizarse con los productos entregables indicados en los incisos a) y b) del Artículo 13. En este reporte se determinan los hallazgos y riesgos que deben ser atendidos por la entidad supervisada, así como la estrategia y actividades de seguimiento que se realizarán.

Asimismo, los resultados de cualquier actividad de supervisión realizada directamente por las superintendencias, se incorporarán en el proceso de supervisión.

Cuando haya una auditoría externa de TI y el o los supervisores se aparten de la opinión emitida por el auditor externo de TI debe incluirse la debida justificación.

El plazo otorgado para remitir a la entidad supervisada el reporte de supervisión sobre los resultados de la auditoría externa, será definido en los Lineamientos Generales.

El supervisor puede declarar inadmisibles los productos entregables indicados en los incisos a) y b) del Artículo 13 cuando incumplan las disposiciones establecidas en este Reglamento o sus Lineamientos Generales. En este caso, la entidad supervisada debe remitir los productos entregables corregidos y realizar la reunión de salida en el plazo indicado en la nota de remisión del reporte de supervisión. Cuando los productos de la auditoría sean admisibles y se incorporen al reporte de supervisión, pero se determinen hallazgos y riesgos, el supervisor debe requerir en la nota de remisión un plan de acción para la gestión de éstos.

Artículo 16. Plan de Acción
La entidad supervisada debe presentar el plan de acción con el formato y plazo establecidos en los Lineamientos Generales.

El plan de acción debe ser aprobado por el Órgano de Dirección de la entidad supervisada y debe estar firmado por su representante legal o gerente general. Las actividades incluidas en el plan de acción deben solventar los hallazgos o mitigar los riesgos indicados en el reporte de supervisión.

Los supervisores pueden hacer observaciones al plan de acción, sugerir mejoras o advertir sobre riesgos significativos. Si a criterio de los supervisores las actividades incluidas en el plan de acción no atienden adecuadamente los hallazgos y riesgos, el plazo solicitado es mayor al razonablemente necesario o la frecuencia de presentación de los informes de avances no permite un adecuado seguimiento al plan de acción, los supervisores deben solicitar las modificaciones pertinentes a la entidad supervisada.

La entidad supervisada debe ejecutar las modificaciones solicitadas por el supervisor y comunicar a éste las variaciones en el plazo requerido. El plan de acción, así modificado, debe ser comunicado al Órgano de Dirección de la entidad supervisada, y debe estar firmado por su representante legal o gerente general.

Las Superintendencias pueden coordinar el reporte y proceso de supervisión.

La aprobación de los planes de acción por parte del supervisor procederá en aquellos casos en que así lo defina su regulación específica.

Sección IV: Prórrogas y calificación de riesgos de TI.

Artículo 17. Prórrogas
La entidad supervisada puede presentar una solicitud de prórroga ante el supervisor, para la remisión de los productos entregables de la auditoría externa de TI o para el plan de acción. El plazo otorgado para presentar una solicitud de prórroga ante el supervisor, a fin de que la misma pueda ser conocida y resuelta por la respectiva superintendencia, será definido en los Lineamientos Generales.

La solicitud debe estar firmada por el representante legal o gerente general de la entidad solicitante y debe indicar la fecha propuesta de remisión de los productos de auditoría externa de TI o acompañarse de un nuevo plan de acción aprobado por su Órgano de Dirección según corresponda. Además, debe contener los motivos y las pruebas, si fuere del caso, que imposibilitan a la entidad para cumplir con el plazo original, y deberá demostrar, que los motivos para su petición se basan en caso fortuito o fuerza mayor, u otras causas fuera de su control.

El superintendente del respectivo órgano supervisor conocerá y valorará los fundamentos presentados y, en los casos que corresponda, otorgará prórroga por escrito, mediante resolución motivada, indicando el plazo adicional concedido. Cuando la unidad de TI es corporativa, las superintendencias coordinarán la concesión de la citada prórroga.

Artículo 18. Calificación de riesgos de TI
El superintendente, cuando corresponda a su modelo de supervisión definido reglamentariamente y aprobado por el CONASSIF, debe emitir la calificación sobre el riesgo de TI de la entidad supervisada. La metodología para determinar dicha calificación se establece en las regulaciones particulares de cada Superintendencia.

Sección V: Bases de datos

Artículo 19. Bases de datos
Las bases de datos actualizadas y las aplicaciones vigentes que procesan o dan acceso a estas bases deben estar accesibles al ente supervisor correspondiente, sin ningún tipo de restricción o condición.

Con este fin, cuando la unidad de TI no forme parte de una entidad supervisada o cuando existan proveedores de TI, la entidad debe establecer un contrato con esa Unidad de TI y con cada uno de los proveedores de TI. Las condiciones que deben observarse en los instrumentos legales en que se pacten los servicios de TI, tendientes a cumplir el objetivo señalado en esta norma, serán definidas en los Lineamientos Generales.

Las bases de datos actualizadas, así como, las aplicaciones vigentes que procesan o dan acceso a estas bases, pueden mantenerse en servicios de computación en la nube, siempre y cuando se cumplan con los requisitos legales, de seguridad y de acceso del supervisor, de acuerdo a la normativa aplicable por cada superintendencia. La respectiva superintendencia puede requerir un modelo de gestión de infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando en estos: la entidad no cumpla los requisitos legales y de seguridad; no se brinde acceso al supervisor; la información que la entidad desea mantener sea sensible o crítica para la continuidad del negocio; la computación en la nube represente un riesgo para el sistema financiero; o cuando afecte los intereses de los clientes.

Disposición transitoria única
De conformidad con el requerimiento dispuesto en el artículo 8. Marco de gestión de TI, las superintendencias deben establecer en los Lineamientos Generales que acompañan este Reglamento una gradualidad para la implementación de los procesos relacionados al marco de gestión de TI. Dicho periodo de gradualidad será de 3 años para las entidades supervisadas por la Superintendencia General de Entidades Financieras y de 5 años para las entidades supervisadas por la Superintendencia General de Valores, Superintendencia de Pensiones y Superintendencia General de Seguros.

Disposiciones derogatorias:
Se deroga el Acuerdo SUGEF-14-09, Reglamento sobre la Gestión de la Tecnología de Información.
Se deroga el Acuerdo de SUGEVAL SGV-A-124. “Acuerdo sobre requerimientos mínimos de tecnología de la información (TI)”.

Disposición final:
Este reglamento rige diez días hábiles después de su publicación en el diario oficial La Gaceta.

II. En lo tocante a las reformas al Reglamento de Auditores Externos aplicable a los sujetos fiscalizados por la SUGEF, SUGEVAL, SUPEN y SUGESE.

considerando que:

1. El segundo párrafo del artículo 119 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558 dispone que, en relación con la operación propia de las entidades fiscalizadas y el registro de las transacciones, la Superintendencia General de Entidades Financieras (en adelante SUGEF) está facultada para dictar las normas generales que sean necesarias para el establecimiento de sanas prácticas bancarias, todo en salvaguarda del interés de la colectividad.

2. El inciso c), del artículo 131 de la Ley N° 7558, establece, como parte de las funciones del Superintendente General de Entidades Financieras, proponer para su aprobación, al Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), las normas que estime necesarias para el desarrollo de las labores de fiscalización y vigilancia. En ese mismo sentido, el numeral ii) del inciso n) de dicho artículo, dispone que el Superintendente General de Entidades Financieras debe proponer al CONASSIF las normas 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, además, faculta a la SUGEF para 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, que den información adecuada al público sobre los intermediarios financieros.

3. El artículo 6 de la Ley Reguladora del Mercado de Valores establece que todas las personas físicas o jurídicas que participen directa o indirectamente en los mercados de valores, deberán inscribirse en el Registro Nacional de Valores e Intermediarios. En ese sentido, dicho artículo dispone que la Superintendencia General de Valores (en adelante SUGEVAL) reglamentará la organización y el funcionamiento del Registro, así como el tipo de información que considere necesaria, suficiente, actualizada y oportuna, todo para garantizar la transparencia del mercado y la protección del inversionista.

4. El artículo 27 "Obligaciones de los proveedores de servicios auxiliares" de la Ley Reguladora del Mercado de Seguros dispone, entre otros, que los auditores externos deben realizar auditorías externas libres de vicios o irregularidades sustanciales o en concordancia con la normativa vigente y los proveedores de servicios auxiliares deben comunicar sobre hechos relevantes y suministrar a la Superintendencia General de Seguros (en adelante SUGESE) la información correcta, completa, dentro de los plazos y las formalidades requeridos. Asimismo, este artículo faculta al CONASSIF a emitir la normativa necesaria que determine el contenido de las obligaciones, la periodicidad, las condiciones, los formatos, los términos, la operatividad y, en general, cualquier aspecto necesario para el efectivo cumplimiento, supervisión, verificación y sanción en caso de inobservancia de estas obligaciones. En ese mismo sentido, los artículos 10 y 30 de la Ley de marras disponen que los auditores externos de las entidades supervisadas deberán poner en conocimiento de la SUGESE, en forma inmediata, las situaciones detectadas que puedan concebirse como operaciones ilegales o pudieren poner en riesgo la estabilidad de la entidad.

5. En el caso de la SUGESE, el artículo 29 de la Ley 8653 que establece las facultades para autorizar y regular a las personas físicas y jurídicas que intervengan en los actos o contratos relacionados con la actividad aseguradora, reaseguradora, la oferta pública y la realización de negocios de seguros con el objeto de velar por la estabilidad y el eficiente funcionamiento del mercado de seguros, así como entregar la más amplia información a los asegurados.

6. Mediante artículo 13, del Acta de la Sesión 893-2010, celebrada el 3 de diciembre del 2010, el Consejo aprobó el "Reglamento de Auditores Externos aplicable a los sujetos fiscalizados por SUGEF, SUGEVAL, SUPEN y SUGESE" cuyo objeto es establecer las disposiciones que regirán para los sujetos supervisados por las superintendencias dirigidas por el Consejo, en la contratación de las firmas de auditorías externas o auditores externos independientes, en los servicios de auditoría.

7. El inciso i) del artículo 171 de la Ley Reguladora del Mercado de Valores establece como una de las funciones del Consejo Nacional de Supervisión del Sistema Financiero reglamentar el intercambio de información que podrán realizar entre sí las diferentes Superintendencias, para el estricto cumplimiento de sus funciones de supervisión prudencial. La Superintendencia que reciba información en virtud de este inciso, deberá mantener las obligaciones de confidencialidad a que está sujeto el receptor inicial de dicha información.

8. El artículo 10 de la Ley 8653, Ley Reguladora del Mercado de Seguros dispone, entre otras potestades del Consejo Nacional, definir mediante reglamento, las normas y los requerimientos del régimen de suficiencia de capital y solvencia que deberán cumplir las entidades aseguradoras y reaseguradoras, para lo cual debe observar hipótesis prudentes y razonables así como prácticas aceptadas internacionalmente que mejor se adapten al mercado de seguros costarricense. En ese sentido, el principio 7.7, de los "Principios básicos de seguros, estándares, guía y metodología de evaluación" de la Asociación Internacional de Supervisores de Seguros exige al Consejo de Administración de la aseguradora que garantice un proceso de presentación de informes financieros confiables, tanto para el público en general como para fines de supervisión. Dispone dicho principio que es importante que el Consejo de Administración salvaguarde y promueva una relación

fluida con el auditor externo, y garantice, entre otros, que los términos de contratación del auditor externo sean claros y adecuados, conforme el alcance de la auditoría y los recursos necesarios para conducirla. Además, dispone que la autoridad supervisora deberá exigir que el auditor externo le notifique cualquier fraude importante, sospecha de fraude importante e incumplimientos regulatorios u otros hallazgos significativos que se desprendan en el proceso de auditoría, así como que el supervisor reciba copia de los informes preparados por el auditor externo de la aseguradora (por ejemplo, cartas de la gerencia).

9. La aplicación de una regulación particular para las entidades supervisadas de acuerdo con su actividad, la complejidad y volumen de las operaciones, el perfil y los sistemas y metodologías de medición del nivel de exposición al riesgo, y el entorno económico, entre otros, requieren que los auditores externos cuenten con los conocimientos técnicos, legales y regulatorios y la experiencia necesaria para llevar a cabo un servicio de esta naturaleza, por lo que es necesario ajustar los requerimientos regulatorios y los requisitos para la inscripción y actualización en el Registro Nacional de Valores e Intermediarios.

10. Los incisos 17 y 13 de los artículos 157 y 159, respectivamente, de la Ley Reguladora del Mercado de Valores y el inciso j del Artículo 46 de la Ley 7523 reformado por la Ley de Protección al Trabajador disponen, en lo que interesa, que las empresas o profesionales que realicen auditorías externas a entidades sujetas a fiscalización de la SUGEVAL, con vicios o irregularidades esenciales que impidan conocer la situación patrimonial o financiera de la entidad auditada, o incumplan las normas contables, no podrán realizar auditorías externas a entidades fiscalizadas por la SUGEVAL, lo cual es aplicable a todas las firmas de auditores externos y a los auditores externos independientes que realicen encargos de auditoría, revisión u otro tipo de labores tipificadas legal o reglamentariamente a los entes supervisados por superintendencias dirigidas por el Consejo, por lo que se convierte en un motivo de desinscripción en el Registro de Auditores Elegibles.

11. El literal c) del artículo 27 de la Ley N° 8653 señala que es obligación de los proveedores de servicios auxiliares de las entidades supervisadas por SUGESE realizar auditorías externas libres de vicios o irregularidades sustanciales o en concordancia con la normativa vigente. Además, dicho artículo dispone que para las obligaciones ahí señaladas, el Consejo y la SUGESE, según corresponda, podrán emitir la normativa necesaria que determine el contenido de las obligaciones, la periodicidad, las condiciones, los formatos, los términos, la operatividad y, en general, cualquier aspecto necesario para su efectivo cumplimiento, supervisión, verificación y sanción en caso de inobservancia.

12. Las disposiciones indicadas en las dos consideraciones anteriores le son aplicables a los auditores externos que presten servicios a todos los entes supervisados de las superintendencias, tal y como lo dispone el segundo párrafo del artículo 19 del "Reglamento de Auditores Externos aplicable a los sujetos fiscalizados por SUGEF, SUGEVAL, SUPEN y SUGESE", en el sentido de que cualquier situación que ponga en riesgo la estabilidad financiera de la entidad auditada debe ser de conocimiento de los entes supervisores, por lo que se hace necesario que exista una comprensión mutua, y cuando sea necesario, oportuno y legalmente aceptable, comunicación entre los supervisores y los auditores externos para llevar a cabo el desempeño de sus responsabilidades.

13. Que la vigilancia preventiva es el mejor recurso con que cuenta el CONASSIF y las Superintendencias para la protección de los intereses del público, siendo estas últimas los organismos encargados de velar por el cumplimiento de las normas legales y de corrección financiera; 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, de manera que los informes y opiniones presentados por los auditores externos se conviertan en información de primera mano para la toma de decisiones por parte de los entes supervisados, los entes supervisores y cuando corresponda, del público en general, por lo que se considera oportuno y necesario reforzar el marco regulatorio, de inscripción y desinscripción en el Registro de Auditores Elegibles en aras de que los profesionales inscritos en dicho registro cuenten con las competencias, presenten la documentación necesaria y conozcan los motivos de desinscripción del registro.

14. Un enfoque de supervisión basado en riesgos, como el que aplican las entidades supervisadas en el ámbito internacional y de implementación por los entes supervisores en nuestro sistema financiero conlleva una revisión crítica de aspectos como el marco normativo, procesos de supervisión, técnicas y habilidades con que el supervisor apoya su labor. Un aspecto medular que caracteriza un desarrollo normativo congruente con este enfoque, consiste en la definición clara de la expectativa del supervisor sobre la calidad de la gestión de las entidades y de la calidad del trabajo que brindan los proveedores de servicios para los entes supervisados, especialmente los auditores externos, debido a que éstos deben contar con un conocimiento técnico, experiencia y equipo de trabajo que le permita desarrollar en el tiempo designado, una evaluación de los controles internos, del cumplimiento normativo, de los riesgos a los que está expuesta la entidad supervisada, lo adecuado de los sistemas de información, la razonabilidad de la información financiera y la aplicación del marco de referencia, entre otros, para emitir una opinión y exponer los resultados de su trabajo, lo cual conlleva desarrollar un trabajo con la excelencia que exigen las normas internacionales, por lo que se requiere dejar explícito que cuando un auditor externo no cumpla con las normas técnicas que le son aplicables o no evidencie exposiciones de riesgo a las que estén expuestas las entidades supervisadas, serán objeto de un proceso administrativo que puede conllevar en su exclusión del Registro de Auditores Elegibles.

15. Los literales b), ñ y o del artículo 171 de la Ley Reguladora del Mercado de Valores dispone que son funciones del Consejo aprobar las normas atinentes a:

    a. la autorización, regulación, supervisión, fiscalización y vigilancia que, conforme a la ley, debe ejecutar la SUGEF,
    b. contabilidad y auditoría, según los principios de contabilidad generalmente aceptados, así como la frecuencia y divulgación de las auditorías externas a que obligatoriamente deberán someterse los sujetos supervisados. En caso de conflicto, estas normas prevalecerán sobre las emitidas por el Colegio de Contadores Públicos de Costa Rica,
    c. la periodicidad, el alcance, los procedimientos y la publicación de los informes rendidos por las auditorías externas de las entidades fiscalizadas, con el fin de lograr la mayor confiabilidad de estas auditorías.

16. Es necesario ajustar las disposiciones del "Reglamento de auditores externos aplicable a los sujetos fiscalizados por la SUGEF, SUGEVAL, SUPEN y SUGESE" con el propósito de hacer la distinción de los requerimientos y obligaciones que aplican específicamente para los auditores externos que prestan servicios a los entes supervisados sobre Tecnología de Información en relación con los auditores externos que prestan servicios sobre auditoría financiera o de cumplimento de Ley 8204 o Riesgos.

17. Mediante artículos 6 y 10 de las actas de las sesiones 1222-2016 y 1223-2016 respectivamente, celebradas el 11 y el 18 de enero del 2016 respectivamente, el CONASSIF resolvió remitir en consulta a las entidades supervisadas y órganos de integración de los sectores regulados, el proyectos de Reglamento General de Gestión de la Tecnología de Información; las reformas al Reglamento de Auditores Externos aplicable a los sujetos fiscalizados por SUGEF, SUGEVAL, SUPEN y SUGESE; y las reformas al Anexo, Lineamientos para la inscripción en el registro de auditores elegibles, para que, en un plazo máximo de veinte días hábiles, contados a partir del día hábil siguiente de recibido el comunicado, enviaran sus comentarios y observaciones; plazo que fue ampliado hasta el 11 de marzo del 2016, según artículos 8 y 14 de las actas de las sesiones 1227-2016 y 1228-2016, celebradas el 2 de febrero del 2016.

Las observaciones recibidas fueron analizadas y en lo correspondiente, incorporadas en el texto final del Reglamento y los Lineamientos Generales.

resolvió:

Reformar el Reglamento de Auditores Externos aplicable a los sujetos fiscalizados por SUGEF, SUGEVAL, SUPEN y SUGESE, de conformidad con el siguiente texto:

1) Reformar el nombre del reglamento para que en adelante se lea **"Reglamento General de Auditores Externos",** y modificar la referencia del nombre en cualquier otra reglamentación aprobada por el Consejo Nacional de Supervisión del Sistema Financiero.

2) Reformar el artículo 1 para que en adelante se lea de la siguiente manera:

Artículo 1. Objeto

Este Reglamento tiene por objeto regular la contratación y la prestación de los servicios de auditoría externa.

3) Reformar el primer y segundo párrafo del artículo 3 para que en adelante se lea de la siguiente manera:

Artículo 3. Auditoría Externa
Los sujetos supervisados deberán someterse a una auditoría externa financiero-contable anual, y a una auditoría externa de tecnologías de la información (TI), ésta última según se establece en el Reglamento General de Gestión de la Tecnología de Información. Ambas auditorías deben estar a cargo, exclusivamente, por firmas de auditorías externas o auditores externos independientes, inscritos en el Registro de Auditores Elegibles que forma parte del Registro Nacional de Valores e Intermediarios, dispuesto en la Ley Reguladora del Mercado de Valores.

En el caso de las auditorías financiero-contables de grupos o conglomerados financieros, todas las entidades domiciliadas en Costa Rica que los conformen deberán ser auditadas por el mismo auditor externo independiente o firma auditora.

4) Reformar el título del Capítulo II y de la Sección I para que en adelante se lea de la siguiente manera:

CAPITULO II

AUDITORES EXTERNOS

Sección I: Requisitos

5) Reformar el título, primer párrafo y literales a) y c) del artículo 5, además adicionar los literales e) y f) a dicho artículo de acuerdo con el siguiente texto:

[…]

Artículo 5. Requisitos generales

La firma de auditoría externa, el socio responsable, el encargado del equipo así como el auditor externo independiente y los miembros del equipo de auditoría deben cumplir los siguientes requisitos:

a. No haber sido declarados insolventes o en quiebra durante los cinco años previos a la contratación.

c. En el caso de la auditoría financiero-contable, la firma de auditoría externa, el socio responsable, el encargado del equipo así como el auditor externo independiente deben estar inscritos y activos en el registro profesional del Colegio de Contadores Públicos de Costa Rica.

e. Para el caso de los auditores de TI, la firma de auditoría externa, el socio responsable y el auditor externo independiente deben reunir los requisitos y experiencia profesional establecidos por las regulaciones

emitidas por la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association/ ISACA).

f. Para el caso de las auditorías de TI, el socio responsable, el encargado del equipo así como el auditor externo independiente, deben contar además con un Certificado CISA vigente (Auditor Certificado de Sistemas de Información por sus siglas en inglés "Certified Information Systems Auditor").

6) Reformar el artículo 6 para que en adelante se lea de la siguiente manera:

Artículo 6. Auditores extranjeros

En el caso de auditorías de entidades domiciliadas en el exterior que formen parte de grupos o conglomerados financieros costarricenses o de entidades domiciliadas en el exterior con sucursal en Costa Rica, la firma auditora del país donde se encuentre domiciliada la entidad deberá cumplir con los siguientes, requisitos:

a. Deberá estar inscrita y activa en el registro profesional del organismo homólogo al colegio profesional correspondiente en Costa Rica, así como en el registro del regulador público correspondiente, en caso de que estos registros existan.

b. Deberá ser representante de una firma que opera internacionalmente y que, a su vez, tenga representación en Costa Rica.

En el caso de emisores de valores domiciliados en el exterior, podrán presentar sus estados financieros auditados por una firma del país de su domicilio, que cumpla el requisito indicado en el inciso a) anterior.

7) Reformar el artículo 7 para que en adelante se lea de la siguiente manera:

Artículo 7. Requisitos de independencia

La independencia del socio responsable, el encargado del equipo o el auditor externo independiente, según corresponda, se comprueba si no forma parte del grupo vinculado a la entidad ni ha formado parte del grupo vinculado durante los períodos a auditar, todo de conformidad con lo establecido en los artículos 6 y 9 del Acuerdo SUGEF 4-04, "Reglamento sobre el grupo vinculado a la entidad".

Sin perjuicio de cualquier otra situación que a juicio de la entidad a auditar o de las firmas de auditorías externas o auditores externos independientes pueda afectar la imparcialidad de éstas, no podrán presentarse en la firma de auditoría, el socio responsable, el encargado del equipo o el auditor independiente, y de conformidad con la especialidad de la auditoría, ninguno de los supuestos que se establecen a continuación:

a. Haber desempeñado cargos en la entidad auditada, sus filiales, asociadas, entidades con cometido especial, subsidiarias o su grupo económico, durante los períodos económicos auditados para el caso de auditoría financiero-contable y durante los dos años anteriores a la contratación para el caso de auditoría en TI.

b. Mantener operaciones de créditos activas, con la entidad auditada, sus accionistas y demás empresas afiliadas.

c. Haber fiscalizado puestos de bolsa como auditor en representación de una bolsa de valores y auditar los estados financieros de los puestos de bolsa por él fiscalizados.

d. Ser agente de bolsa en ejercicio.

e. Formar parte de organismos de administración de la entidad auditada.

f. Mantener oficinas comerciales dentro de las instalaciones de la entidad regulada.

g. Ser proveedor de servicios auxiliares de seguros autorizado de la entidad aseguradora durante los períodos económicos auditados.

Adicionalmente, las firmas de auditorías externas o auditores externos independientes deben cumplir con las obligaciones y deberes establecidos en las leyes reguladoras de los colegios profesionales respectivos y los principios éticos rectores de su profesión.

8) Reformar el artículo 8 para que en adelante se lea de la siguiente manera:

Artículo 8. Prestación de servicios complementarios

La firma de auditoría externa o auditor externo independiente puede prestar los servicios de auditoría, cuando no haya prestado servicios complementarios en forma directa o a través de una empresa vinculada, de forma que podría comprometer su independencia.

Para el caso de auditoría financiero-contable, el plazo de esta restricción comprende el período del acuerdo o compromiso de auditoría y el período cubierto por los estados financieros a auditar. En el caso de la auditoría en TI, el plazo de esta restricción comprende los dos años anteriores a la fecha de notificación del requerimiento de la auditoría y durante su realización. No se consideran dentro del alcance de este artículo los servicios requeridos expresamente por alguna disposición normativa aprobada por el CONASSIF.

Entre los servicios complementarios que se consideran comprometen la independencia, se encuentran los siguientes:

a. Para el caso de la auditoría financiero-contable:
   i. Contabilidad y otros servicios relacionados con los registros contables o estados financieros de la entidad supervisada.
   ii. Diseño e implementación de sistemas de información financiera.
   iii. Estimación o valoración.
   iv. Actuariales.
   v. Auditoría Interna.
   vi. Asesoría en materia de riesgos.
   vii. De dirección o recursos humanos.
   viii. Asesor de inversiones o servicios de banco de inversiones.
   ix. Legales y asesoramiento especializado con la auditoría.
   x. Cualquier otro servicio que la Superintendencia respectiva considere que interfiere con la independencia del auditor, para lo cual deberá dictar una resolución motivada.

b. Para el caso de la auditoría en TI:
   i. Diagnóstico, implementación y mantenimiento de marcos de control sobre TI.
   ii. Asesoría en riesgos en TI.
   iii. Capacitación en TI.
   iv. Consultoría en TI.
   v. Cualquier otro servicio que la Superintendencia respectiva considere que interfiere con la independencia del auditor, para lo cual deberá dictar una resolución motivada.

Para efectos de la determinación de la existencia de una compañía vinculada, a la firma de auditoría externa o auditor externo independiente, se considerará la definición de parte relacionada, contenida en los artículos 6 y 9 del Acuerdo SUGEF 4-04, “Reglamento sobre el grupo vinculado a la entidad”.

9) Reformar el primer párrafo del artículo 9 para que en adelante se lea de la siguiente manera:

Artículo 9. Ingresos
La remuneración de la firma de auditoría externa o auditor externo independiente no podrá depender de las condiciones o resultados de su trabajo de auditoría. Tampoco podrá pactarse sobre la base del resultado financiero del período a que se refieren los estados contables sujetos a la auditoría o del resultado de la valoración del gobierno y de la gestión en TI.

10) Incluir un literal l) adicional a las motivaciones de desinscripción en el artículo 12 desinscripción del registro:

l. Presenten documentos y otros entregables que impidan conocer de forma veraz el estado de los procesos de gobierno y de gestión de TI de una entidad supervisada.

11) Modificar los párrafos uno y dos del artículo 13 para que en adelante se lea de la siguiente manera:

Artículo 13. Verificación del cumplimiento de requisitos
De previo a la suscripción del contrato por los servicios de auditoría, la entidad supervisada debe comprobar que el prestatario de los servicios cumple con los requisitos establecidos en los artículos 5, 7, 8, y en los artículos 6 y 10 cuando correspondan, de este Reglamento.

Posteriormente, con la presentación de los informes de auditoría, la entidad supervisada debe verificar el requisito establecido en el Artículo 9 de este Reglamento, por medio de:

12) Modificar el segundo párrafo del artículo 14 para que en adelante se lea de la siguiente manera:

La comunicación deberá realizarse, a más tardar, en el caso de la auditoría financiero-contable el 30 de junio de cada año, tratándose de empresas que realizan sus cierres en diciembre de cada año, y el 30 de abril para las que lo realizan en otra fecha de corte. En el caso de la auditoría en TI, debe realizarse en el plazo de veinte días hábiles posteriores a la contratación respectiva.

13) Derogar el artículo 22 e incluir una disposición final única para la entrada en vigor de los cambios:

Disposición final única. Entrada en vigor.
Rige a partir de su publicación en el Diario Oficial La Gaceta.

III. Reformar el Anexo: Lineamientos para la inscripción en el registro de auditores elegibles, según el siguiente detalle:

a. Modificar el primer párrafo de la Sección A "Documentación mínima" y los literales d), e) y h) de conformidad con el siguiente texto:

Los profesionales o firmas auditoras deben presentar la solicitud de inscripción, especificando el área en la cual desarrollaran su actividad (financiero-contable, tecnologías de información, o ambas), acompañadas de los documentos originales indicados a continuación. Solamente se dará trámite a las solicitudes que incorporen la documentación completa.

d. Certificación extendida por el Colegio de Contadores Públicos o del Colegio de Profesionales en Informática y Computación según corresponda, donde conste que el profesional independiente es miembro activo. Dicha certificación deberá ser presentada para cada uno de los socios que conforman la firma, y para los encargados directos de la auditoría de conformidad con lo establecido en el artículo 5 inciso c) de este Reglamento.

e. En el caso de firmas de auditoría que soliciten inscribirse en el área financiero-contable deberán presentar certificación de que es miembro activo de Colegio de Contadores Públicos.

h. Estar al día en el pago de sus obligaciones con la Caja Costarricense de Seguro Social de conformidad con los artículos 74 y 74 bis.- de la Ley Constitutiva de la Caja Costarricense de Seguro Social (Ley 17). Asimismo, estar al día en el pago de sus obligaciones con el Fondo de Desarrollo Social y Asignaciones Familiares.

b. Modificar los literales c), e), y la información incluida en el cuadro al final del literal f) de la Sección B "Documentación general del profesional o firma de auditoría" de conformidad con el siguiente texto:

c. Estructura organizativa de la firma y del departamento de auditoría. En el departamento de auditoría se deberá identificar los diferentes niveles jerárquicos para cada una de las áreas financiero-contables y de tecnología de información.

e. Descripción general del sistema de control de calidad aplicado por la firma que asegure la calidad de los trabajos realizados, así como las políticas y procedimientos que garanticen el adecuado cumplimiento de los colegios profesionales respectivos y los principios éticos rectores de su profesión. Para las auditorías financiero-contables, las políticas y procedimientos de la firma deben garantizar el cumplimiento del Reglamento de Ética Profesional y del Código de Ética de los Contadores Profesionales, emitido por la Federación Internacional de Contadores.

f. […]

Responsable		**Detalle**
Nombre de entidad supervisada		
Cantidad de periodos de servicios de auditoría externa		
Área de servicio (financiero-contable o tecnología de información)		
Profesional Independiente	Nombre Completo	
	Cantidad de periodos[(a)]	
Gerente	Nombre Completo	
	Cantidad de periodos[(a)]	
Encargado	Nombre Completo	
	Cantidad de periodos[(a)]	
Socio 1	Nombre Completo	
	Cantidad de periodos[(a)]	
Socio 2	Nombre Completo	
	Cantidad de periodos[(a)]	
Socio 3	Nombre Completo	
	Cantidad de periodos[(a)]	
(a) Corresponde a la cantidad de periodos en que el funcionario ha participado en los servicios de auditoría externa brindados a la entidad supervisada por la SUGEF, SUGEVAL, SUPEN o SUGESE.		

c. Modificar los literales a), c), d) e), g) y h) de la Sección C1 "Declaración jurada rendida por el socio que firma el dictamen y representante legal de la firma auditora" de conformidad con el siguiente texto:

a. No he sido declarado insolvente o en quiebra durante los cinco años anteriores a la fecha de solicitud de inscripción.

c. Mi representada cumple con los requisitos y experiencia profesional o independencia establecidos en los artículos 5, 6 y 7 del Reglamento General de Auditores Externos.

d. Mi representada no ha incumplido durante los últimos dos años con el procedimiento de comunicación de sustitución establecido en el artículo 15 del Reglamento General de Auditores Externos.

e. Con base en un proceso de debida diligencia y debidamente documentado, declaro que ninguno de los miembros que conforman el equipo de auditoría de mi representada han sido declarados insolventes durante los cinco años anteriores a la fecha de solicitud de inscripción, ni han sido condenados por delitos contra la fe pública o la propiedad durante los últimos diez años por autoridades judiciales competentes.

g. Como socio de la firma tengo una experiencia mínima de [número de años] años de laborar como socio, y como encargado de equipo en auditorías en [detallar el área de auditoría y el tipo de entidades] o en el sector [detallar los sectores en los que tiene experiencia].

h. La firma auditora cuenta con políticas y procedimientos que aseguran el control de la calidad de todos los trabajos de auditoría realizados. Dichas políticas y procedimientos internos permiten verificar, de manera adecuada, el cumplimiento de las leyes reguladoras y sus reglamentos de los colegios profesionales respectivos y los principios éticos rectores de la profesión.

d. Modificar los literales a), c), d) e), f), g) y h) de la Sección C2 "Declaración jurada rendida por el profesional independiente" de conformidad con el siguiente texto:

a. No he sido declarado insolvente o en quiebra durante los cinco años anteriores a la fecha de solicitud de inscripción.

c. Cumplo con los requisitos y experiencia profesional o independencia establecidos en los artículos 5, y 7 del Reglamento General de Auditores Externos.

d. No he incumplido durante los últimos dos años con el procedimiento de comunicación de sustitución establecido en el artículo 15 del Reglamento General de Auditores Externos.

e. Con base en un proceso de debida diligencia y debidamente documentado, declaro que ninguno de los miembros que conforman el equipo de auditoría han sido declarados insolventes durante los cinco años anteriores a la fecha de solicitud de inscripción, ni han sido condenados por delitos contra la fe pública o la propiedad durante los últimos diez años por autoridades judiciales competentes.

f. Con base en un proceso de debida diligencia y debidamente documentado, declaro que se ha procedido a la rotación, de al menos cada cinco años, del encargado y miembros del equipo asignado en la auditoría externa anual.

g. Como profesional independiente tengo una experiencia mínima de [número de años] años de laborar, y como encargado de equipo en auditorías en [detallar el área de auditoría y el tipo de entidades] o en el sector [detallar los sectores en los que tiene experiencia].

h. Como profesional independiente cuento con políticas y procedimientos que aseguran el control de la calidad de todos los trabajos de auditoría realizados. Dichas políticas y procedimientos internos permiten verificar de manera adecuada el cumplimiento de las leyes reguladoras y sus reglamentos de los colegios profesionales respectivos y los principios éticos rectores de la profesión.

e. Modificar el segundo párrafo de la Sección C3 "Declaración jurada del folleto informativo del profesional independiente o de la firma auditora" de conformidad con el siguiente texto:

Que con fundamento en un proceso de debida diligencia, el folleto informativo del [Contador Público o Profesional en Informática] con páginas numeradas de la 1-xx a xx-xx, presentado a la Superintendencia General de Valores es exacto, veraz, verificable, suficiente, y fue preparado para efectos del registro de auditores elegibles de las Superintendencias en cumplimiento de lo establecido en el Reglamento General de Auditores Externos.

f. Modificar los apartados A "Datos generales", C"Cursos o seminarios de especialización", D "Experiencia en servicios de Auditoría Externa" y E "Otra experiencia laboral" de la Sección D "Actualización" de conformidad con el siguiente texto:

A "Datos generales"

Nombre completo	
Número de identificación	
Teléfono oficina	
E-Mail	
Número de identificación del Colegio Profesional respectivo	
Posición actual en la firma [(a)]	

(a)Si el profesional ejercerá las funciones de auditoría externa en forma independiente, deberá indicarlo mediante la denominación "Independiente"

C "Cursos o seminarios de especialización"

Cursos o seminarios que tengan relación directa con las empresas en que el socio, gerente, encargado o profesional independiente pretende prestar los servicios de auditoría externa.

Nombre o descripción del curso	Año de conclusión
1)	
2)	
3)	
4)	
5)	

D "Experiencia en servicios de Auditoría Externa"

Firma de profesionales en que ha laborado [(a)]	Área (financiero contable o TI en la que ha laborado)	Posición (socio, gerente o encargado)	Años de ocupar la posición	Sectores en que posee experiencia en auditoría [(b)]	Años de experiencia en auditoría del sector financiero	Detalle de Empresas que ha auditado

Si el profesional ha ejercido las funciones de auditoría externa en forma independiente, deberá indicarlo mediante la denominación "Independiente".

(b) Los sectores deben especificarse, haciendo mención, al menos a los siguientes: sector bancario, sector cooperativo, sector financiero no bancario, sector de seguros, fideicomisos emisores, universalidades, intermediarios de valores, otros participantes del mercado de valores; y en el caso de empresas no financieras: sector de comercio y servicios, industria y construcción, y agricultura, caza y pesca.

E "Otra experiencia laboral"

Nombre de la Empresa	**Posición**	**Inicio** (mes-año)	**Fin** (mes-año)	**Breve descripción de labores desempeñadas**

g. Añadir una disposición adicional, para que se lea de la siguiente manera:

Disposiciones adicionales

Disposición adicional única
Las firmas de auditorías externas o auditores externos independientes que al momento de entrada en vigencia de la reforma al Reglamento de Auditores Externos aplicable a los sujetos fiscalizados por SUGEF, SUGEVAL, SUPEN y SUGESE, que se encuentren inscritos en el registro de auditores elegibles, y que deseen inscribirse para brindar los servicios de auditoría de TI, deberán complementar los requisitos establecidos en los literales e) y f) del artículo 5 de dicho cuerpo normativo. Para lo anterior, deben presentar el trámite correspondiente según el proceso definido en el artículo 11 del Reglamento, específicamente los puntos a), d), g) y h) de la Sección A y los puntos c) y d) de la Sección B que se indican en el Anexo de este Reglamento y sean atinentes a lo dispuesto a auditores de TI.

Disposición final única:
Las anteriores disposiciones rigen a partir de su publicación en el Diario Oficial "La Gaceta".

Atentamente,

Documento suscrito mediante firma digital.

Jorge Monge Bonilla
Secretario del Consejo

***Comunicado a**: Sistema Financiero Nacional, Diario Oficial La Gaceta (c. a: Superintendencias, Auditoría Interna).*