CONSEJO NACIONAL DE SUPERVISIÓN DEL
SISTEMA FINANCIERO

REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

APROBADO POR EL CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO, MEDIANTE ARTÍCULO 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.

PUBLICADO EN EL ALCANCE 80 DEL DIARIO OFICIAL “LA GACETA”, DEL 17 DE ABRIL DE 2017.

RIGE 10 DÍAS HÁBILES DESPUÉS DE SU PUBLICACIÓN EN EL DIARIO OFICIAL “LA GACETA”

Versión	Referencia
1.0	Así modificado por medio del Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 6, de las actas de las sesiones 1602-2020 y 1604-2020, celebradas el 31 de agosto y 7 de setiembre de 2020, publicado en La Gaceta N° 230 del miércoles 16 de setiembre del 2020.

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

Señores
Sistema Financiero Costarricense y
Otras Entidades Financieras

Estimados señores:

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 a este Reglamento. Cuando el informe sea preparado por profesionales que ejercen la profesión de Contador Público Autorizado, deberá presentarse por medios electrónicos de conformidad con los

procedimientos de emisión mediante firma digital establecidos por el Colegio de Contadores Públicos de Costa Rica.[1]
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

[1] Así modificado por medio del Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 6, de las actas de las sesiones 1602-2020 y 1604-2020, celebradas el 31 de agosto y 7 de setiembre de 2020, publicado en La Gaceta N° 230 del miércoles 16 de setiembre del 2020.

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.