CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

ACUERDO CONASSIF 5-17

(antes Acuerdo Sugef 14-17) *

REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante 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. Publicado en el Alcance No 80 del diario oficial La Gaceta No 71 del 17 de abril del 2017. Rige diez días hábiles después de su publicación en el diario oficial La Gaceta.

VER CONSIDERANDOS DEL REGLAMENTO

VER REGLAMENTO

VER LINEAMIENTOS GENERALES

VER HISTORIAL DE CAMBIOS

Versión documento	Fecha de actualización
6	1° de enero de 2023

* El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 9 de las actas de las sesiones 1725-2022 y 1726-2022, celebradas el 18 de abril del 2022, dispuso en firme modificar la nomenclatura de los reglamentos con alcance transversal. Rige a partir de su publicación en La Gaceta. Publicado en el Alcance 83 a La Gaceta 78 del viernes 29 de abril del 2022.

TABLA DE CONTENIDO

CONSIDERANDOS

El Consejo Nacional de Supervisión del Sistema Financiero, mediante 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:

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 de 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 de 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 adapte 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 los 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 la 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

[5a]Artículo 1. Objeto

Este Reglamento establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades y empresas 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.

e) [5b] Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados, en los casos en que así lo requiere el supervisor responsable.

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 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) [4]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.

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.

REGRESAR AL INICIO

LINEAMIENTOS GENERALES

Circular Externa
31 de marzo de 2017
SGF-1033-2017
SGF-PUBLICO

Superintendencia General de Entidades Financieras. Despacho del Superintendente. Santa Ana, del 31 de marzo del 2017.

El Superintendente de Entidades Financieras,

Considerando que:

1. El Consejo Nacional de Supervisión del Sistema Financiero, mediante 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, aprobó el *Reglamento General de Gestión de la Tecnología de Información*, Acuerdo CONASSIF 5-17 [5].

2. Conforme el artículo 4 del Reglamento, corresponde a los Superintendentes emitir conjuntamente los *Lineamientos Generales* para su aplicación;

3. Los artículos 8, 9, 10, 11, 12, 13, 14, 15 16, 17, 19, el transitorio único, el formulario de perfil tecnológico, la solicitud sobre tipo de gestión de TI, los criterios complementarios para la ejecución de la auditoría externa de TI e informe, la matriz de evaluación, la periodicidad del reporte supervisor, y el formato del plan de acción del citado reglamento, requieren la emisión de lineamientos en relación al marco de gestión de TI.

4. El *Reglamento General de Gestión de la Tecnología de Información*, Acuerdo CONASSIF 5-17 [5], así como, sus *Lineamientos Generales*, aplican para las entidades supervisadas por la Superintendencia General de Valores (SUGEVAL), la Superintendencia de Pensiones (SUPEN), la Superintendencia General de Seguros (SUGESE) y la Superintendencia General de Entidades Financieras (SUGEF).

5. El anterior Acuerdo SUGEF 14-09 *"Reglamento sobre la gestión de la tecnología de información"* y sus Lineamientos Generales, que aplicaban únicamente para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras (SUGEF); están siendo derogados.

Dispone:

1. ***Emitir los "Lineamientos Generales al Reglamento General de Gestión de la Tecnología de Información," de conformidad con el siguiente texto:***

LINEAMIENTOS GENERALES AL REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

1. Marco de gestión de TI y periodo de transición (Artículo 8 y transitorio único)

De los procesos detallados en el Anexo 1, las entidades supervisadas deberán determinar cuáles resultan adecuados a su Marco de Gestión de TI, todo debidamente fundamentado y aprobado por su Órgano de Dirección.

Las entidades deben implementar los procesos de su marco de gestión de TI gradualmente como máximo durante los primeros 3 años para las entidades supervisadas por SUGEF y 5 años para el resto de las entidades supervisadas por las otras Superintendencias, contados a partir de la entrada en vigencia del reglamento.

En concordancia con la naturaleza, modelo de negocio, criticidad de los procesos y dependencia tecnológica de información y la complejidad de sus operaciones, las superintendencias esperan que los entes supervisados implementen los órganos, comités, instancias y controles, para lo cual deben contar con una estructura organizacional para la gestión de TI que delimite claramente sus obligaciones, funciones y responsabilidades y que cuente con políticas orientadas a cautelar una adecuada gestión de TI en congruencia con la estrategia de gestión de los riesgos de TI determinada por las entidades supervisadas.

Algunos aspectos relevantes a tomar en consideración para el establecimiento de los roles y responsabilidades de las partes interesadas para la implementación, supervisión y evaluación de la gestión de TI son los siguientes:

Órgano de Dirección.

i. Aprobar el Marco de Gestión de TI.

ii. Direccionar a sus miembros, alta gerencia, líder del área de informática y el líder de administrar los riesgos, o cualquier otro miembro que se considere pertinente

para que se involucren en las instancias que les permitan gestionar las tecnologías de información.

iii. Establecer un Comité de TI, cuando así lo requiera de acuerdo a su ordenamiento organizacional y la naturaleza de sus operaciones.

iv. Designar la firma de auditores externos o profesional independiente de TI, de conformidad con la propuesta que para esos efectos le presenten las instancias correspondientes.

v. Establecer, aprobar y supervisar la aplicación de las políticas de gestión de TI.

vi. Aprobar las estrategias y la designación de los recursos necesarios para la implementación del Marco de Gestión de TI.

vii. Analizar y aprobar los informes de la Auditoría Externa de TI que se remitan a las respectivas superintendencias.

viii. Orientar la implementación de las actividades que son responsabilidad del Comité de TI en caso que no establezca ese comité en su estructura organizacional.

Comité de TI

Cuando la entidad supervisada establezca un Comité de TI dentro de su estructura organizacional, su conformación debe ser acorde a las mejores prácticas y le corresponderán, entre otras funciones, las siguientes:

i. Velar por la implementación de los procesos de la gestión de TI.

ii. Asesorar en la formulación de las estrategias, metas de TI y velar por su cumplimiento.

iii. Proponer las políticas generales con base en el marco de gestión de TI.

iv. Recomendar las prioridades para las inversiones en TI.

v. Proponer los niveles de tolerancia al riesgo de TI en congruencia con el perfil tecnológico de la entidad.

vi. Velar por que la gerencia gestione el riesgo de TI en concordancia con las estrategias y políticas aprobadas.

vii. Analizar el Plan de Acción y sus ajustes que atiendan el reporte de supervisión de TI.

viii. Dar seguimiento a las acciones contenidas en el Plan de Acción.

Alta Gerencia.

i. Proponer al Órgano de Dirección las estrategias y los recursos requeridos para la implementación del marco de Gestión de TI.

ii. Proponer al Órgano de Dirección o Comité de TI, en caso de existencia de este último, la firma de auditores externos o profesional independiente de TI para la ejecución de la Auditoría Externa de TI.

iii. Implementar y controlar la ejecución de las políticas y procedimientos de gestión de TI.

iv. Designar las áreas de negocio responsables de implementar los procesos del marco de Gestión TI.

iv. Atender todos los requerimientos de información que formule el supervisor.

2. Perfil tecnológico (Artículo 9)

El "*Perfil Tecnológico*" y la "*Guía para la descarga, llenado y remisión del Perfil Tecnológico*" vigentes, se encuentran en los sitios electrónicos oficiales de cada superintendencia.

El formato del archivo del perfil tecnológico y su medio de remisión, serán comunicados por la respectiva Superintendencia.

El plazo de remisión del perfil tecnológico, se define en el punto 10 de estos lineamientos.

3. Tipo de gestión de TI (Artículo 10)

La solicitud de validación del tipo de gestión de TI debe contener una justificación debidamente sustentada del por qué se considera que el modelo de la gestión de TI es corporativa, considerando una descripción detalla de al menos los aspectos siguientes:

i. **Gestión de recursos:** cómo se realiza la gestión y asignación de los recursos de TI, a las diferentes entidades supervisadas. Estos recursos pueden incluir a los

colaboradores, requerimientos de hardware, software, sistemas de información, seguridad de la información y telecomunicaciones.

ii. **Formulación de políticas y procedimientos:** cómo se definen las políticas y procedimientos a nivel corporativo, para orientar las decisiones y los procesos de TI, dentro de cada una de las entidades supervisadas.

iii. **Aspectos financieros:** cómo se realiza la aplicación de la coordinación que se realiza para establecer los presupuestos, el control de la ejecución presupuestaria y la aplicación de las directrices presupuestarias.

iv. **Esquema de coordinación:** cómo se dan las actividades de coordinación entre las diferentes entidades supervisadas, para analizar los temas relacionados con requerimientos, reportes, niveles de servicio y seguimiento y cumplimiento de objetivos. El esquema de toma de decisiones y el organigrama.

v. **Aspectos de control:** cuál es el esquema que se establece para el control de los procesos de TI entre las entidades supervisadas.

vi. **Plataforma tecnológica:** describir cómo la plataforma tecnológica es compartida por las diferentes entidades supervisadas, tanto a nivel de hardware como de software.

vii. **Servicios de TI brindados por terceros:** en el caso que las entidades soporten sus servicios de tecnologías de información a través de terceros, se deben incluir el contrato y las referencias de su aprobación entre la entidad y el proveedor que presta el servicio.

4. Criterios complementarios para la ejecución de la auditoría (Artículos 11 y 12)

El tipo de auditoría externa de TI requerida es una auditoría directa que brinde un alto nivel, pero no absoluto, de aseguramiento acerca de la efectividad de los controles sobre los procesos y debe involucrar al menos lo siguiente:

1. Planificación del trabajo a realizar, identificando los recursos requeridos.

2. Evaluación de la efectividad del diseño de los procedimientos de control.

3. Prueba de la efectividad operativa de los procedimientos de control.

4. Formulación de una conclusión sobre el diseño y la efectividad operativa de los procedimientos de control.

5. Formato del informe de auditoría externa de TI (Artículo 13)

El informe de auditoría externa de TI debe estar debidamente numerado y foliado. Debe contener el formato indicado seguidamente:

Carátula del Informe

a. Nombre de la entidad supervisada.

b. Nombre de las Superintendencias que recibirán los resultados de la auditoría externa de TI.

c. Título del informe: "Auditoría externa de TI".

d. Número de oficio en que el supervisor de la entidad solicita la auditoría.

e. Nombre del Auditor (*Firma, socio responsable y encargado del equipo o auditor externo independiente*) y el correspondiente código del certificado CISA.

f. Fecha de finalización del informe.

Secciones del Informe

I. Generalidades de la auditoría externa.

a. Identificación de la entidad supervisada.

1. Tipo de entidad supervisada (*entidad individual o grupo de entidades*).

2. Tipo de gestión de TI (*individual o corporativa*).

3. Otros aspectos importantes a criterio del auditor.

b. Restricción.

Indicar las restricciones con respecto a la circulación del informe.

c. Equipo de auditoría.

Integración del equipo de auditoría:

1. Nombre completo.

2. Rol dentro del equipo.

d. Período de ejecución de la auditoría.

e. Período auditado.

II. Alcance de la Auditoría

Detalle del alcance de la auditoría.

III. Limitaciones Generales

Indique las limitaciones generales a que estuvo sujeta la auditoría.

IV. Resultados de la auditoría

a. Opinión General.

b. Conclusiones.

Para cada proceso evaluado se debe indicar lo siguiente:

i. los hallazgos determinados durante la auditoría,

ii. los riesgos de TI a que está expuesto la entidad supervisada a raíz de los hallazgos señalados en el punto anterior,

iii. las recomendaciones de solución a los riesgos de TI señalados en el punto anterior.

c. Comentarios de la gerencia al borrador de informe (documento formal y firmado que contiene los comentarios de la gerencia sobre los hallazgos y su aceptación o rechazo).

d. Detalle de cualquier reserva que el auditor externo de TI tuviese en cuanto al alcance de la auditoría.

V. Firmas

El informe debe estar firmado al menos por el socio responsable o el auditor externo independiente.

VI. Anexos

El informe debe contener como mínimo los anexos siguientes:

1. Matriz de calificación de la gestión de TI. (de la entidad supervisada y de los proveedores de TI).

2. Número del acuerdo del órgano directivo, en el cual aprueba el informe final de la auditoría externa de TI.

3. Índice de documentación de los papeles de trabajo referenciados en el informe de auditoría externa de TI y en la matriz de calificación de gestión de TI con explicaciones detalladas de los documentos.

4. Cualquier otra información o documento considerado necesario por el auditor externo de TI.

6. Matriz de evaluación (Artículo 13)

La matriz de evaluación de la gestión de TI contiene los criterios que serán evaluados para cada proceso.

La entidad supervisada debe entregar la matriz de evaluación de la gestión de TI al Auditor externo de TI, para que la misma sea llenada durante el proceso de ejecución de la auditoría.

La "Matriz de evaluación de la gestión de TI", en su versión vigente, y la "Guía para completar la Matriz de evaluación gestión de TI'' se encuentran en los sitios electrónicos oficiales de cada superintendencia.

7. Contenido mínimo de la presentación de salida (Artículo 14)

El contenido mínimo de la presentación de salida es el siguiente:

a. Objetivos de la auditoría.

b. Metodología utilizada en el proceso de revisión.

c. Alcance de la auditoría.

d. Período auditado.

e. Periodo de ejecución de la auditoría.

f. Hallazgos relevantes por proceso.

g. Riesgos de TI relevantes.

h. Opinión general.

i. Recomendaciones.

8. Formato del plan de acción (Artículo 16)

Los planes de acción deben especificar claramente la acción a implementar, su duración o plazo de ejecución, las fechas de inicio y fin de ejecución, el responsable, los indicadores para medir la efectividad de las acciones tomadas para mitigar el riesgo o corregir el hallazgo y una explicación clara de que tales acciones van a lograr lo propuesto.

El plan de acción en su versión vigente y la "*Guía para la descarga, llenado y remisión del Plan de Acción*" se encuentran en los sitios electrónicos oficiales de cada superintendencia.

9. Bases de datos (Artículo 19)

Con el fin de mantener la continuidad del servicio que brinda la unidad de TI cuando no forme parte de una entidad supervisada y/o los proveedores de TI contratados por la entidad; los contratos que se establezcan, deberán contener la cláusula siguiente:

"Artículo XX. Obligaciones de la unidad de TI/proveedor de TI frente a los supervisores de las entidades.

(nombre de la unidad de TI/proveedor de TI) se obliga a suministrar a (nombre de la Superintendencia) y al auditor externo de TI toda información que le sea requerida por estos, así como, todas las facilidades requeridas en la supervisión de TI, de acuerdo con la reglamentación emitida por el Consejo Nacional de Supervisión del Sistema Financiero de la República de Costa Rica y sus Lineamientos Generales.

Asimismo, (nombre de la unidad de TI/proveedor de TI) se obliga a continuar brindando los servicios de TI contratados aún en el caso de intervención de alguna entidad supervisada por parte de un órgano supervisor costarricense."

10. Plazos (Artículos 9, 10, 12, 14, 15, 17)

Los plazos para los diferentes productos que serán generados para la implementación del Reglamento General de Gestión de la Tecnología de Información, son los siguientes:

a. *Tipo de gestión de TI:* Las solicitudes remitidas por las entidades para que su gestión de TI sean tipificadas como corporativas, deben ser resueltas por las Superintendencias en el plazo de veinte días hábiles contados a partir de la recepción de la solicitud y su documentación completa.

   En caso que las Superintendencias requieran información complementaria para atender la solicitud, suspende el plazo de resolución.

b. *Perfil Tecnológico:* El perfil tecnológico, debe ser remitido anualmente.

c. *Plazo de ejecución de la auditoría:* El plazo otorgado para la remisión de los productos entregables de la auditoría externa de tecnologías de información no debe ser mayor a nueve meses; adicionalmente, las Superintendencias pueden requerir en un plazo menor esos productos de acuerdo a la definición de riesgo que represente la entidad para la supervisión.

   La entidad supervisada puede presentar una solicitud de prórroga ante el supervisor, a más tardar veinte días hábiles antes del vencimiento del plazo para la remisión de los productos entregables de la auditoría externa de TI, a fin de que la misma pueda ser conocida y resuelta por la respetiva superintendencia.

d. *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 en el plazo de cinco días hábiles contados a partir del recibo de los productos de la auditoría por parte del supervisor.

e. *Reporte de Supervisión:* Las superintendencias deben remitir a la entidad supervisada el reporte de supervisión en el plazo de veinte días hábiles contados a partir de la reunión de salida para presentar los resultados de la auditoría externa, salvo cuando los supervisores soliciten cambios al informe de auditoría externa, en cuyo caso el plazo inicia con la entrega definitiva del informe.

f. *Plan de Acción:*

   i. La entidad supervisada puede presentar una solicitud de prórroga ante el supervisor, de conformidad con los plazos que para el efecto dispone la Ley General de Administración Pública, a fin de que la misma pueda ser conocida y resuelta por la respetiva superintendencia.

   ii. El plan de acción debe incluir la frecuencia de presentación de los informes de avance con plazos no mayores a los seis meses.

Anexo 1: Procesos del Marco de Gestión de TI

No.	Aspectos del Marco de Gestión de TI	Descripción	Años para su implementación posterior a la entrada en vigencia del reglamento								
			Entidades supervisadas por SUGEVAL, SUPEN, SUGESE					SUGEF			
			1	2	3	4	5	A la entrada en vigencia	1	2	3
1.1	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	X						X		
1.2	Asegurar la Entrega de Beneficios	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costos aceptables.	X						X		
1.3	Asegurar la Optimización del Riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	X						X		
1.4	Asegurar la Optimización de Recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	X						X		
1.5	Asegurar la Transparencia hacia las Partes Interesadas	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	X						X		
2.1	Gestionar el Marco de Gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	X					X			

No.	Aspectos del Marco de Gestión de TI	Descripción	Años para su implementación posterior a la entrada en vigencia del reglamento								
			Entidades supervisadas por SUGEVAL, SUPEN, SUGESE					SUGEF			
			1	2	3	4	5	A la entrada en vigencia	1	2	3
2.2	Gestionar la Estrategia	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	X					X			
2.3	Gestionar la Arquitectura Empresarial	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costos potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.				X				X	
2.4	Gestionar el Portafolio	Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.				X				X	
2.5	Gestionar el Presupuesto y los Costos	Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, costo y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costos a la empresa. Consultar a las partes interesadas para identificar y controlar los costos totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.			X			X			

No.	Aspectos del Marco de Gestión de TI	Descripción	Años para su implementación posterior a la entrada en vigencia del reglamento								
			Entidades supervisadas por SUGEVAL, SUPEN, SUGESE					SUGEF			
			1	2	3	4	5	A la entrada en vigencia	1	2	3
2.6	Gestionar los Recursos Humanos	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.				X				X	
2.7	Gestionar las relaciones	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.				X					X
2.8	Gestionar los acuerdos de servicio	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.	X					X			
2.9	Gestionar los Proveedores	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados, minimizando el riesgo que los proveedores no cumplan.	X					X			
2.10	Gestionar la Calidad	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.					X				X
2.11	Gestionar el Riesgo	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial.		X				X			
2.12	Gestionar la Seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.		X				X			

No.	Aspectos del Marco de Gestión de TI	Descripción	Años para su implementación posterior a la entrada en vigencia del reglamento								
			Entidades supervisadas por SUGEVAL, SUPEN, SUGESE					SUGEF			
			1	2	3	4	5	A la entrada en vigencia	1	2	3
3.1	Gestión de Programas y Proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.	X					X			
3.2	Gestionar la Definición de Requisitos	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.				X				X	
3.3	Gestionar la Identificación y Construcción de Soluciones	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores / fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.			X			X			
3.4	Gestionar la Disponibilidad y la Capacidad	Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.			X			X			
3.5	Gestionar los Cambios	Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.		X				X			
3.6	Gestionar la Aceptación del Cambio y la Transición	Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.				X				X	

No.	Aspectos del Marco de Gestión de TI	Descripción	Años para su implementación posterior a la entrada en vigencia del reglamento								
			Entidades supervisadas por SUGEVAL, SUPEN, SUGESE					SUGEF			
			1	2	3	4	5	A la entrada en vigencia	1	2	3
3.7	Gestionar los Activos	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.			X					X	
3.8	Gestionar la Configuración	Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.			X			X			
4.1	Gestionar Operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.			X			X			
4.2	Gestionar Peticiones e Incidentes de Servicio	Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	X					X			
4.3	Gestionar Problemas	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.			X			X			
4.4	Gestionar la Continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.		X				X			

No.	Aspectos del Marco de Gestión de TI	Descripción	Años para su implementación posterior a la entrada en vigencia del reglamento								
			Entidades supervisadas por SUGEVAL, SUPEN, SUGESE					SUGEF			
			1	2	3	4	5	A la entrada en vigencia	1	2	3
4.5	Gestionar Servicios de Seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.		X				X			
4.6	Gestionar Controles de Proceso de Negocio	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.		X					X		
5.1	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.					X				X
5.2	Supervisar, Evaluar y Valorar el Sistema de Control Interno	Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.		X				X			
5.3	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general. Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.					X				X

Rigen a partir de la publicación en el Diario Oficial La Gaceta, del Acuerdo CONASSIF 5-17[5] "Reglamento General de Gestión de la Tecnología de Información".

Aprobado por el Comité de Superintendentes.

Atentamente,

Documento suscrito mediante firma digital.

Javier Cascante Elizondo

Superintendente

GAA/gvl*

CIRCULAR EXTERNA

SGF-2985-2020 SP-1120-2020 SGS-C-0013-2020 SGV-1534

02 de setiembre 2020

Dirigida a:

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;

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.

Asunto: Informar al Sistema Financiero Nacional sobre las fechas y grupos de entidades para el envío del Perfil Tecnológico del Acuerdo CONASSIF 5-17 [5] "Reglamento para la Gestión de Tecnologías de Información".

Los Superintendentes Generales de Entidades Financieras, Pensiones, Valores y Seguros,

Considerando que:

1. El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) aprobó el *"Reglamento General de Gestión de la Tecnología de Información"*, mediante 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.

2. Los Lineamientos Generales del Reglamento General de Gestión de la Tecnología de Información fueron emitidos el 28 de marzo de 2017.

3. El artículo 9 *Perfil Tecnológico* del Reglamento en referencia, señala que cada entidad supervisada debe elaborar y mantener actualizado su perfil tecnológico y que cuando la unidad de TI es corporativa se debe remitir un único perfil y coordinar que ese perfil tecnológico se ajuste al marco de gestión de TI. Además, establece que el perfil tecnológico debe identificar las particularidades de cada una de las entidades integrantes del grupo o conglomerado financiero a las cuales les aplica.

4. El numeral 2 Perfil Tecnológico (Artículo 9) de los Lineamientos Generales del Reglamento General de Gestión de la Tecnología de Información, establece que el formato del archivo del perfil tecnológico y su medio de remisión, serán comunicados por la respectiva Superintendencia.

5. El artículo 10 de los "*Lineamientos Generales al Reglamento General de Gestión de la Tecnología de Información,"* establece que el perfil tecnológico debe ser remitido anualmente.

6. Las entidades supervisadas requieren conocer los aspectos a cumplir en la preparación del archivo de remisión del Perfil Tecnológico.

7. El Sistema de Captura, Verificación y Carga de Datos (SICVECA) desarrollado por SUGEF, es el medio para la recepción del Perfil Tecnológico definido en el Acuerdo CONASSIF 14-17 [5], excepto para el caso de las entidades supervisadas por SUGESE.

8. A las entidades de Pensiones se comunicaron las disposiciones para la remisión del Perfil Tecnológico mediante el oficio SP-A-189-2017 del 31 de octubre del 2017.

Disponen:

Emitir los siguientes aspectos referentes a la preparación del archivo de remisión del Perfil Tecnológico y la definición de grupos de entidades para su envío.

1. La estructura y archivos necesarios para la completitud del Perfil Tecnológico se encuentran disponibles en el sitio Web de cada Superintendencia, a saber:

Superintendencia	Sitio Web
SUGEF	https://www.sugef.fi.cr/informacion_relevante/manuales/manual_de_informacion_sicveca.aspx
SUGEVAL	www.sugeval.fi.cr
SUGESE	www.sugese.fi.cr https://www.sugese.fi.cr/seccion-marco-legal/acuerdos-superintendente/acuerdos-conjuntos-superintendencia
SUPEN	www.supen.fi.cr

2. La estructura de los archivos tipo XML para el formato del Perfil Tecnológico está diseñada sobre archivos XSD. Las entidades podrán utilizar la herramienta Infopath para el llenado de la información requerida.

3. El archivo tipo XLSX es el formato del Perfil Tecnológico para las entidades supervisadas por SUGESE.

4. Para SUGEF, SUGEVAL y SUPEN, el medio de remisión del Perfil Tecnológico es el sistema SICVECA, utilizando la clase de datos 24 “Perfil Tecnológico”.

5. Para SUGESE, las entidades supervisadas, deberán realizar la remisión oficial del Perfil Tecnológico considerando los lineamientos establecidos en el SGS-0678-2019 del 28 de

junio de 2019, lo anterior, sin perjuicio de que el Superintendente General de Seguros defina a futuro mediante acuerdo general otro medio de remisión.

6. Las fechas y grupos de entidades para la remisión del Perfil Tecnológico, se detallan en el Anexo 1. Estas fechas y grupos de entidades podrán ser modificadas ante variaciones en las prioridades de supervisión, mediante carta de la respectiva Superintendencia en el caso de entidades con gestión de TI individual.

7. Para efectos de la remisión del Perfil Tecnológico, en lo relativo al tipo de gestión de TI, se reitera que, si la gestión de TI de las entidades es individual, deberán remitir un perfil tecnológico por cada entidad supervisada, excepto que se haya autorizado la solicitud para que su gestión sea considerada corporativa, en cuyo caso deben remitir un único Perfil Tecnológico para las entidades del grupo o conglomerado a las cuales se autorizó la gestión corporativa.

Rige a partir del 4 de enero del 2021.

Atentamente,

Documento suscrito mediante firma digital.

José Armando Fallas Martínez
Superintendente General de Entidades Financieras a. í.

Documento suscrito mediante firma digital.

María Lucía Fernández Garita
Superintendente General de Valores

Documento suscrito mediante firma digital.

Tomás Soley Pérez
Superintendente General de Seguros

Documento suscrito mediante firma digital.

Rocío Aguilar Montoya
Superintendente General de Pensiones

Anexo

Distribución y fechas de recepción del Perfil Tecnológico

Grupo 1: ENERO

Fecha	Descripción	Entidades
Primeros 10 días hábiles de ENERO	**Mutuales de Ahorro y Crédito**	
	Conglomerado Financiero Grupo Mutual Alajuela – La Vivienda de Ahorro y Préstamo	1. Grupo Mutual Alajuela – La Vivienda de Ahorro y Préstamo (SUGEF) 2. Mutual Sociedad de Fondos de Inversión S.A. (SUGEVAL) 3. Mutual Valores Puesto de Bolsa S.A.(SUGEVAL)
	Mutual Cartago de Ahorro y Préstamo	1. Mutual Cartago de Ahorro y Préstamo (SUGEF)
	Otras Entidades Financieras	

Fecha	Descripción	Entidades
	Conglomerado Financiero Caja de Ahorro y Préstamos de la ANDE	1. Caja de Ahorro y Préstamos de la ANDE (SUGEF) 2. Vida Plena Operadora de Planes de Pensiones Complementarias S.A. (SUPEN) 3. Caja de Ande Seguros Sociedad Agencia de Seguros, S.A.
	Bancos Creados Por Leyes Especiales Conglomerado Financiero Banco Popular y de Desarrollo Comunal	1. Banco Popular y de Desarrollo Comunal (SUGEF) 2. Operadora de Planes de Pensiones Complementarias del Banco Popular y de Desarrollo Comunal S.A.(SUPEN) 3. Popular Sociedad de Fondos de Inversión S.A.(SUGEVAL) 4. Popular Valores Puesto de Bolsa S.A. (SUGEVAL)
	Bancos Privados Grupo Financiero Davivienda	1. Banco Davivienda (Costa Rica) S.A (SUGEF) 2. Davivienda Puesto de Bolsa (Costa Rica) S.A. (SUGEVAL) 3. Davivienda Seguros Costa Rica, S.A. (SUGESE)
	Grupo Financiero Citibank	1. Banco CMB (Costa Rica) S.A. (SUGEF) 2. Citi Valores Accival S.A.(SUGEVAL)
	Grupo Financiero Improsa	1. Banco Improsa S.A. (SUGEF) 2. Improsa Sociedad Administradora de Fondos de Inversión S.A. (SUGEVAL) 3. Improsa Valores Puesto de Bolsa S.A. (SUGEVAL)
	Grupo Financiero Lafise	1. Banco LAFISE S.A. (SUGEF) 2. Seguros Lafise Costa Rica S.A. (SUGESE) 3. LAFISE Valores Puesto de Bolsa S.A. (SUGEVAL)
	Regímenes de Capitalización Colectiva Fondos complementarios creados por leyes especiales o convenciones colectivas	1. Fondo de Empleados del ICE. 2. Fondo del Banco Nacional de Costa Rica.
	Aseguradoras Best Meridian Insurance Company	1. Best Meridian Insurance Company (SUGESE)
	Triple- S Blue Inc. (Atlantic Southern Insurance Company-Sucursal En Costa Rica)	1. Triple- S Blue Inc. (Atlantic Southern Insurance Company-Sucursal en Costa Rica) (SUGESE)
	Aseguradora Sagicor Costa Rica S.A.	1. Aseguradora Sagicor Costa Rica S.A. (SUGESE)
	Grupo INS	1. Instituto Nacional De Seguros (SUGESE) 2. INS Valores Puesto de Bolsa S.A. (SUGEVAL) 3. INS Inversiones Sociedad Administradora de Fondos de Inversión S.A. (SUGEVAL)
	Organizaciones Cooperativas de Ahorro y Crédito Grupo Financiero Alianza	1. Coopealianza R.L. (SUGEF)
	Cooperativas	1. Coopavegra R.L. (SUGEF) 2. Coopeamistad R.L. (SUGEF) 3. Coopeande No.1 R.L. (SUGEF) 4. Coopeaya R.L. (SUGEF) 5. Coopebanpo R.L. (SUGEF) 6. Coopecaja R.L. (SUGEF) 7. Coopecar R.L. (SUGEF)

Grupo 2: ABRIL

Fecha	Descripción	Entidades
Primeros 10 días hábiles de ABRIL	**Bancos Comerciales del Estado**	
	Conglomerado Financiero Banco de Costa Rica	1. Banco de Costa Rica (SUGEF) 2. BCR Pensión Operadora de Planes de Pensiones Complementarias S.A.(SUPEN) 3. BCR Sociedad Administradora de Fondos de Inversión S.A. (SUGEVAL) 4. BCR Valores S.A. (SUGEVAL)
	Bancos Privados	
	Grupo Financiero Banco BCT S.A.	1. Banco BCT S.A.(SUGEF) 2. BCT Sociedad de Fondos de Inversión S.A. (SUGEVAL) 3. BCT Valores Puesto de Bolsa S.A. (SUGEVAL)
	Grupo Financiero Prival	1. Prival Bank (Costa Rica) S.A. (SUGEF) 2. Prival Securities (Costa Rica), Puesto de Bolsa S.A. (SUGEVAL) 3. Prival Sociedad Administradora de Fondos de Inversión, S.A. (SUGEVAL)
	Banco Promerica de Costa Rica S.A.	1. Banco Promerica de Costa Rica S.A. (SUGEF)
	Grupo Financiero BNS de Costa Rica	1. Scotiabank de Costa Rica S.A. (SUGEF) 2. Scotia Sociedad de Fondos de Inversión S.A. (SUGEVAL)
	Puestos de Bolsa y Sociedades de Fondos de Inversión	
	Grupo Bursátil Aldesa S.A.	1. Aldesa Puesto de Bolsa S.A.(SUGEVAL) 2. Aldesa Sociedad de Fondos de Inversión S.A. (SUGEVAL) 3. Aldesa Fideicomisos S.A. (SUGEVAL) 4. Grupo Bursátil Aldesa S.A. (SUGEVAL)
	Grupo Financiero Mercado de Valores	1. Mercado de Valores de Costa Rica Puesto de Bolsa S.A. (SUGEVAL) 2. Multifondos de Costa Rica Sociedad de Fondos de Inversión S.A. (SUGEVAL) 3. Grupo Financiero Mercado de Valores de Costa Rica S.A. (SUGEVAL)
	Grupo Financiero Acobo	1. Acobo Puesto de Bolsa S.A. (SUGEVAL) 2. Vista Sociedad de Fondos de Inversión S.A. (SUGEVAL) 3. Corporación Acobo S.A. (SUGEVAL) 4. Servicios Fiduciarios Acobo S.A. (SUGEVAL)
	Grupo Empresarial Sama	1. Inversiones SAMA S.A. (SUGEVAL) 2. SAMA Sociedad de Fondos de Inversión GS, S.A. (SUGEVAL) 3. Grupo Empresarial Sama S.A. (SUGEVAL)
	Bolsas y Depositarios de Valores	
	Bolsa Nacional de Valores S.A. y Subsidiarias	1. Bolsa Nacional de Valores S.A. (SUGEVAL) 2. Interclear Central de Valores S.A. (SUGEVAL)
	Banco Central de Costa Rica	1. Sistema de Anotación en Cuenta de Deuda Pública del Banco Central de Costa Rica (SUGEVAL).
	Aseguradoras	
	Seguros del Magisterio S.A.	1. Seguros del Magisterio S.A. (SUGESE)
	Aseguradora Del Istmo (Adisa) S.A.	1. Aseguradora Del Istmo (Adisa) S.A. (SUGESE)
	Oceánica De Seguros S.A.	1. Oceánica De Seguros S.A. (SUGESE)

Fecha	Descripción	Entidades
	Qualitas Compañía De Seguros (Costa Rica), S.A.	1. Qualitas Compañía De Seguros (Costa Rica), S.A. (SUGESE)
	Organizaciones Cooperativas De Ahorro Y Crédito Grupo Financiero Coocique **Cooperativas**	 1. Coocique R.L. (SUGEF) 1. Coopefyl R.L. (SUGEF) 2. Coopegrecia R.L. (SUGEF) 3. Coopejudicial R.L. (SUGEF) 4. Coopelecheros R.L. (SUGEF) 5. Coopemédicos R.L. (SUGEF) 6. Coopemep R.L. (SUGEF) 7. Coopesanmarcos R.L. (SUGEF)
	Operadoras de Pensiones	1. Operadora de Pensiones de la Caja Costarricense del Seguro Social
	Regímenes de Capitalización Colectiva Fondos complementarios creados por leyes especiales o convenciones colectivas	 1. Fondo del retiro de empleados de la CCSS. 2. Fondo de Vendedores de Lotería.

Grupo 3: AGOSTO

Fecha	Descripción	Entidades
Primeros 10 días hábiles de AGOSTO	**Bancos Comerciales del Estado** Conglomerado Financiero Banco Nacional de Costa Rica	1. Banco Nacional de Costa Rica (SUGEF) 2. BN Sociedad Administradora de Fondos de Inversión S.A. (SUGEVAL) 3. BN Valores Puesto de Bolsa S.A. (SUGEVAL) 4. BN Vital Operadora de Planes de Pensiones Complementarias S.A. (SUPEN)
	Bancos Creados Por Leyes Especiales Banco Hipotecario de la Vivienda	1. Banco Hipotecario de la Vivienda (SUGEF)
	Bancos Privados Grupo Financiero BAC Credomatic Banco Cathay de Costa Rica S.A. Banco General (Costa Rica) S.A.	1. Banco BAC San José S.A.(SUGEF) 2. BAC San José Pensiones Operadora de Pensiones Complementarias S.A. (SUPEN) 3. BAC San José Puesto de Bolsa S.A.(SUGEVAL) 4. BAC San José Sociedad de Fondos Inversión S.A. (SUGEVAL) 1. Banco Cathay de Costa Rica S.A. (SUGEF) 1. Banco General (Costa Rica) S.A (SUGEF)
	Empresas Financieras No Bancarias Grupo Financiero Cafsa **Financieras**	1. Financiera Cafsa S.A. (SUGEF) 1. Financiera Comeca S.A. (SUGEF) 2. Financiera Desyfin S.A. (SUGEF) 3. Financiera Gente, S.A.(SUGEF) 4. Financiera Credilat, S.A. (SUGEF)
	Proveedores de Precios Latín Vector S.A. Proveedor Integral de Precios Centroamérica S.A. Valmer Costa Rica S.A.	1. Latín Vector S.A. (SUGEVAL) 1. Proveedor Integral de Precios Centroamérica S.A. (SUGEVAL) 1. Valmer Costa Rica S.A. (SUGEVAL)
	Aseguradora Pan American Life Insurance de Costa Rica, S.A. Mapfre | Seguros Costa Rica S.A. Assa Compañía de Seguros, S.A.	1. Pan American Life Insurance De Costa Rica, S.A. (SUGESE) 1. Mapfre | Seguros Costa Rica S.A. (SUGESE) 1. Assa Compañía De Seguros, S.A. (SUGESE)
	Organizaciones Cooperativas De Ahorro y Crédito Grupo Financiero Coopenae CS Grupo Financiero **Cooperativas**	1. Coopenae R.L. (SUGEF) 1. Coopeservidores R.L. (SUGEF) 1. Coopesanramón R.L. (SUGEF) 2. Coopeuna R.L. (SUGEF) 3. Credecoop R.L. (SUGEF)
	Regímenes de Capitalización Colectiva Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social.	1. Fondo del Poder Judicial.

Fecha	Descripción	Entidades
	Regímenes de Capitalización Colectiva Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social.	1. Regímenes de Capitalización Colectiva del Magisterio Nacional.

HISTORIAL DE CAMBIOS

Versión 1: Texto del *Reglamento General de Gestión de la Tecnología de Información*, aprobado por el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), mediante 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. Este Reglamento rige diez días hábiles después de su publicación en el diario oficial La Gaceta. Pendiente de publicación en el "Diario Oficial La Gaceta".

Texto de los Lineamientos Generales al Reglamento General de Gestión de la Tecnología de Información, aprobados según Circular Externa SGF-1033-2017 SGF-PUBLICO, Superintendencia General de Entidades Financieras. Despacho del Superintendente. Santa Ana, del 31 de marzo del 2017.

Versión 2: *Reglamento General de Gestión de la Tecnología de Información*, publicado en el Alcance Nº 80 del diario oficial La Gaceta Nº 71 del 17 de abril del 2017. Este Reglamento rige diez días hábiles después de su publicación en el diario oficial La Gaceta.

Versión 3: CIRCULAR EXTERNA SGF-2985-2020; SP-1120-2020; SGS-C-0013-2020; SGV-1534 del 02 de setiembre 2020. Asunto: Informar al Sistema Financiero Nacional sobre las fechas y grupos de entidades para el envío del Perfil Tecnológico del Acuerdo CONASSIF 5-17[5] "Reglamento para la Gestión de Tecnologías de Información".

Versión 4: Modifica el inciso a) del "Artículo 13. Productos entregables". Modificación aprobada en firme por el 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. Rige a partir de su publicación en el Diario Oficial La Gaceta. Publicado en el Diario Oficial La Gaceta Nº 230 del miércoles 16 de setiembre del 2020.

Versión 5: *****El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 9 de las actas de las sesiones 1725-2022 y 1726-2022, celebradas el 18 de abril del 2022, dispuso en firme modificar la nomenclatura de los reglamentos con alcance transversal. Rige a partir de su publicación en La Gaceta. Publicado en el Alcance 83 a La Gaceta 78 del viernes 29 de abril del 2022.

*****El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 5 y 6 de las actas de las sesiones 1759-2022 y 1760-2022, celebradas el 26 de setiembre del 2022, dispuso:

[5a] Reformar el Artículo 1. Objeto.

[5b] Adicionar un literal e) al Artículo 2. Alcance.

Rige a partir del 1° de enero de 2023. Publicado en el Alcance 222 a La Gaceta 198 del martes 18 de octubre de 2022.

Versión 06: Entrada en vigor de los cambios aprobados por el Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 5 y 6 de las actas de las sesiones 1759-2022 y 1760-2022, celebradas el 26 de setiembre del 2022. Rige a partir del 1° de enero de 2023. Publicado en el Alcance 222 a La Gaceta 198 del martes 18 de octubre de 2022.