El Superintendente General de Entidades Financieras, el Superintendente General de Valores, el Superintendente de Pensiones y el Superintendente General de Seguros, a las 9:00 horas del 28 de marzo de 2017,

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 SUGEF 14-17.

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 SUGEF-14-17, 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.

Disponen:

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.
v. 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	

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
2.5	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			
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

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
2.11	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			
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			

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
3.5	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	
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			

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
4.2	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			
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

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
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

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

ANEXO
LINEAMIENTOS PARA LA INSCRIPCIÓN EN EL REGISTRO DE AUDITORES ELEGIBLES Y ACTUALIZACIÓN DE INFORMACIÓN

En el presente anexo, se establecen los requisitos que deberán cumplir los profesionales o firmas auditoras que deseen prestar servicios de auditoría externa a sujetos fiscalizados por las Superintendencias, para su inscripción en el Registro Nacional de Valores e Intermediarios.

SECCIÓN A
DOCUMENTACIÓN MÍNIMA

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

Las certificaciones solicitadas no deberán tener un plazo mayor al mes de emitidos. Toda la documentación será de carácter confidencial. Los documentos adicionales aportados y no solicitados en este Reglamento no serán considerados en el proceso de inscripción.

Las solicitudes deben ser presentadas a la Superintendencia General de Valores, la cual a su vez las comunicará a las otras Superintendencias en el momento que se reciban. La Superintendencia General de Valores, a solicitud de las personas interesadas, emitirá una certificación de que el profesional independiente o la firma auditora están inscritos en el Registro.

a) Solicitud de inscripción del profesional independiente o las firmas auditoras. La solicitud deberá ser firmada por el profesional independiente o su apoderado, o el representante legal en caso de las firmas auditoras, y deberá ser autenticada por notario público. Cuando la solicitud se haga por medio de

representantes legales o apoderados, deberá adjuntarse la correspondiente certificación de personaría jurídica o del mandato, expedida por el Registro Público Nacional o Notario Público. La solicitud deberá indicar una dirección permanente para atender notificaciones o comunicaciones.

b) Declaración jurada rendida por el representante legal de la firma o el profesional independiente donde se indiquen todas las sociedades relacionadas, por propiedad o control, con el profesional, la firma, o los socios que prestan servicios de auditoría externa, así como las actividades que realizan.
c) Documentación general del profesional o firma de auditoría de conformidad con lo establecido en la sección B este anexo.
d) Certificación extendida por el Colegio de Contadores Públicos o del Colegio de Profesionales en Informática y Computación según corresponda, donde conste que el profesional independiente es miembro activo. Dicha certificación deberá ser presentada para cada uno de los socios que conforman la firma, y para los encargados directos de la auditoría de conformidad con lo establecido en el artículo 5 inciso c) de este Reglamento.
e) En el caso de firmas de auditoría que soliciten inscribirse en el área financiero-contable deberán presentar certificación de que es miembro activo de Colegio de Contadores Públicos.
f) Certificación registral o notarial de los poderes conferidos a cada uno de los socios en el caso de firmas auditoras.
g) Declaración jurada rendida por el representante legal de la firma o el profesional independiente, del cumplimiento de los requisitos y experiencia profesional establecidos en los artículos 5, 6 y 7 de este Reglamento, así como en las secciones A y B del presente anexo. En las secciones C1 y C2 de este anexo se definen los contenidos mínimos de esta declaración.
h) [2] Estar al día en el pago de sus obligaciones con la Caja Costarricense de Seguro Social de conformidad con los artículos 74 y 74 bis de la Ley Constitutiva de la Caja Costarricense de Seguro Social (Ley 17). Asimismo, estar al día en el pago de sus obligaciones con el Fondo de Desarrollo Social y Asignaciones Familiares. ,

SECCIÓN B
DOCUMENTACIÓN GENERAL DEL PROFESIONAL O FIRMA DE AUDITORÍA

El profesional o la firma auditora deberán presentar sus atestados, los cuales deberán incluir como mínimo la siguiente información:

a) Identificación del profesional o la firma auditora, conteniendo los siguientes datos: razón social o nombre de la persona física, tipo de sociedad o Asociación, domicilio legal, teléfono, fax, correo electrónico, y otros datos relevantes que la identifiquen.
b) Fecha de constitución de la firma.
c) Estructura organizativa de la firma y del departamento de auditoría. En el departamento de auditoría se deberá identificar los diferentes niveles jerárquicos para cada una de las áreas financiero-contables y de tecnología de información.
d) Currículo de los socios y profesionales habilitados para firmar los informes de auditoría y de los profesionales que ocupan el cargo de gerente o encargado de la auditoría que laboran para una firma. Éste deberá contener al menos: datos personales, número de años de experiencia como socio, gerente o encargado de compromiso en el sector financiero y en otros sectores. Debe utilizar como base el formato establecido en el Apartado I, de la sección D de este Anexo.
e) Descripción general del sistema de control de calidad aplicado por la firma que asegure la calidad de los trabajos realizados, así como las políticas y procedimientos que garanticen el adecuado cumplimiento de los colegios profesionales respectivos y los principios éticos rectores de su profesión. Para las auditorías financiero-contables, las políticas y procedimientos de la firma deben garantizar el cumplimiento del Reglamento de Ética Profesional y del Código de Ética de los Contadores Profesionales, emitido por la Federación Internacional de Contadores.
f) Detalle de los clientes que son sujetos fiscalizados por alguna de las superintendencias a la fecha de la presentación del documento general del profesional o firma de auditoría. Para cada cliente deberá indicar: Nombre del cliente, períodos de servicios prestados en auditoría externa, socio, gerente y encargado responsable de los servicios prestados a la fecha de la solicitud de inscripción. La información debe presentarse de acuerdo el siguiente formato:

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

g) En el caso de que la firma cuente con algún respaldo internacional deberá indicar el tipo de corresponsalía obtenida y representaciones que ejerce la firma.

La documentación general del profesional o firma de auditoría deberá venir acompañada de una declaración jurada rendida por el representante legal de la firma o el profesional independiente mediante la cual garantiza la veracidad de la información proporcionada. En la sección C3 de este anexo se define el contenido mínimo de esta declaración.

SECCIÓN C
CONTENIDO MÍNIMO DE DECLARACIONES

C. 1 DECLARACIÓN JURADA RENDIDA POR EL SOCIO QUE FIRMA EL DICTAMEN Y REPRESENTANTE LEGAL DE LA FIRMA AUDITORA

Yo [*Nombre del representante legal de la firma auditora*] [*Carnet No. XXXX*] declaro bajo fe de juramento:

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

b) No me encuentro sujeto a una sanción de conformidad con lo establecido en el inciso 17 del artículo 157 y el inciso 13 del artículo 159 de la Ley Reguladora del Mercado de Valores, Ley 7732, y el inciso j del artículo 46 de la Ley 7523 reformado por la Ley de Protección al Trabajador por haber rendido informes de auditorías de entidades sujetas a fiscalización con vicios o irregularidades esenciales que impidieron conocer la situación patrimonial o financiera de la entidad auditada o porque incumplieron las normas de contabilidad establecidas por el Consejo Nacional de Supervisión del Sistema Financiero.
c) Mi representada cumple con los requisitos y experiencia profesional o independencia establecidos en los artículos 5, 6 y 7 del Reglamento General de Auditores Externos.
d) Mi representada no ha incumplido durante los últimos dos años con el procedimiento de comunicación de sustitución establecido en el artículo 15 del Reglamento General de Auditores Externos.
e) Con base en un proceso de debida diligencia y debidamente documentado, declaro que ninguno de los miembros que conforman el equipo de auditoría de mi representada han sido declarados insolventes durante los cinco años anteriores a la fecha de solicitud de inscripción, ni han sido condenados por delitos contra la fe pública o la propiedad durante los últimos diez años por autoridades judiciales competentes.
f) Con base en un proceso de debida diligencia y debidamente documentado declaro que se ha procedido a la rotación, al menos cada cinco años, del encargado y miembros del equipo asignado en la auditoría externa anual.
g) Como socio de la firma tengo una experiencia mínima de [*número de años*] años de laborar como socio y como encargado de equipo en auditorías en [*detallar el área de auditoría y el tipo de entidades*] o en el sector [*detallar los sectores en los que tiene experiencia*].
h) La firma auditora cuenta con políticas y procedimientos que aseguran el control de la calidad de todos los trabajos de auditoría realizados. Dichas políticas y procedimientos internos permiten verificar, de manera adecuada, el cumplimiento de las leyes reguladoras y sus reglamentos de los colegios profesionales respectivos y los principios éticos rectores de la profesión.
i) No tengo operaciones de créditos activas con la entidad auditada, sus accionistas y demás empresas afiliadas.

Es todo. Leído lo anterior al compareciente, lo aprueba y firma en (*LUGAR*) a las (*HORA*) horas del (*DÍA*) de (*MES*) de (*AÑO*). FIRMA.

C 2. DECLARACIÓN JURADA RENDIDA POR EL PROFESIONAL INDEPENDIENTE

Yo [*Nombre del profesional independiente*) [*Carnet No. XXXX*] declaro bajo fe de juramento:

a) No he sido declarado insolvente o en quiebra durante los cinco años anteriores a la fecha de solicitud de inscripción.
b) No me encuentro sujeto a una sanción de conformidad con lo establecido en el inciso 17 del artículo 157 y el inciso 13 del artículo 159 de la Ley Reguladora del Mercado de Valores, Ley 7732, y el inciso j del artículo 46 de la Ley 7523 reformado por la Ley de Protección al Trabajador por haber rendido informes de auditorías de entidades sujetas a fiscalización con vicios o irregularidades esenciales que impidieron conocer la situación patrimonial o financiera de la entidad auditada o porque incumplieron las normas de contabilidad establecidas por el Consejo Nacional de Supervisión del Sistema Financiero.
c) Cumplo con los requisitos y experiencia profesional o independencia establecidos en los artículos 5 y 7 del Reglamento General de Auditores Externos.
d) No he incumplido durante los últimos dos años con el procedimiento de comunicación de sustitución establecido en el artículo 15 del Reglamento General de Auditores Externos.
e) Con base en un proceso de debida diligencia y debidamente documentado, declaro que ninguno de los miembros que conforman el equipo de auditoría han sido declarados insolventes durante los cinco años anteriores a la fecha de solicitud de inscripción, ni han sido condenados por delitos contra la fe pública o la propiedad durante los últimos diez años por autoridades judiciales competentes.
f) Con base en un proceso de debida diligencia y debidamente documentado, declaro que se ha procedido a la rotación, de al menos cada cinco años, del encargado y miembros del equipo asignado en la auditoría externa anual.
g) Como profesional independiente tengo una experiencia mínima de [*número de años*] años de laborar y como encargado de equipo en auditorías en [*detallar el área de auditoría y el tipo de entidades*] o en el sector [*detallar los sectores en los que tiene experiencia*].
h) Como profesional independiente cuento con políticas y procedimientos que aseguran el control de la calidad de todos los trabajos de auditoría realizados. Dichas políticas y procedimientos internos permiten verificar de manera adecuada el cumplimiento de las leyes reguladoras y sus reglamentos de los colegios profesionales respectivos y los principios éticos rectores de la profesión.
i) No tengo operaciones de crédito activas con la entidad auditada, sus accionistas y demás empresas afiliadas.

Es todo. Leído lo anterior al compareciente, lo aprueba y firma en (*LUGAR*) a las (*HORA*) horas del (*DÍA*) de (*MES*) de (*AÑO*). FIRMA

C 3. DECLARACIÓN JURADA DEL FOLLETO INFORMATIVO DEL PROFESIONAL INDEPENDIENTE O DE LA FIRMA AUDITORA

Yo [*Nombre del profesional independiente o del representante legal de la firma auditora*] [*Carnet No. XXXX*] declaro bajo fe de juramento:

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

Es todo. Leído lo anterior al compareciente, lo aprueba y firma en (*LUGAR*) a las (*HORA*) horas del (*DÍA*) de (*MES*) de (*AÑO*). FIRMA

SECCIÓN D
ACTUALIZACIÓN

En el momento en que cambien las condiciones en que fue otorgada la inscripción del auditor externo independiente o la firma auditora en el Registro Nacional de Valores e Intermediarios, el auditor externo independiente o la firma auditora deberá remitir los cambios correspondientes, en un plazo de 5 días hábiles posteriores a la fecha del evento, con una declaración ante notario público de que los cambios en mención son los únicos que se han presentado hasta la fecha.

En caso de que no se presenten cambios, al 30 de marzo de cada año el representante legal de la firma o el profesional independiente deberá presentar una declaración ante notario público en la cual manifieste que las condiciones actuales sobre las que se otorgó resolución de inscripción como auditor elegible en el Registro Nacional de Valores e Intermediarios no han variado.

Apartado I

A. DATOS GENERALES

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

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

B. ESTUDIOS

Grado académico	Carrera	Especialidad	Fecha de certificado	
			Mes	Año

C. CURSOS O SEMINARIOS DE ESPECIALIZACIÓN

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

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

D. EXPERIENCIA EN SERVICIOS DE AUDITORÍA EXTERNA

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

(a) Si el profesional ha ejercido las funciones de auditoría externa en forma independiente, deberá indicarlo mediante la denominación "Independiente".
(b) Los sectores deben especificarse, haciendo mención, al menos a los siguientes: sector bancario, sector cooperativo, sector financiero no bancario, sector de seguros, fideicomisos emisores, universalidades, intermediarios de valores, otros participantes del mercado de valores; y en el caso de empresas no financieras: sector de comercio y servicios, industria y construcción, y agricultura, caza y pesca.

E. OTRA EXPERIENCIA LABORAL

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

Rigen a partir de la publicación en el Diario Oficial La Gaceta, del Acuerdo SUGEF 14-17 "Reglamento General de Gestión de la Tecnología de Información".