27 de noviembre del 2023

CNS-1834/04

CNS-1835/05

Señor

Alberto Dent Zeledón, *Presidente*

***Consejo Nacional de Supervisión del Sistema Financiero***

Estimado señor:

El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 4 y 5 de las actas de las sesiones 1834-2023 y 1835-2023, celebradas el 20 de noviembre del 2023,

**considerando que:**

1. El numeral 2 del artículo 361 de la *Ley General de la Administración Pública*, Ley 6227, establece que se concederá a las entidades representativas de intereses de carácter general o corporativo afectadas por la disposición, la oportunidad de exponer su parecer.
2. Se elaboró el *Reglamento General de Gobierno y Gestión de la Tecnología de Información*, en cumplimiento del *Procedimiento para la Tramitación ante el Consejo Nacional de Supervisión del Sistema Financiero Costarricense de proyectos de emisión o reforma de reglamentos del sistema financiero*, el cual debe ser sometido en consulta a las entidades supervisadas, cámaras y gremios, así como a los grupos y conglomerados financieros.

**dispuso en firme:**

remitir en consulta, en cumplimiento de lo establecido en el numeral 2, artículo 361, de la *Ley General de la Administración Pública*, Ley 6227, al sistema financiero nacional y a la Asociación Costarricense de Auditores en Informática, la propuesta de modificación al *Reglamento General de Gestión de la Tecnología de Información*, Acuerdo Conassif 5-17, en el entendido que, en un plazo máximo de quince días hábiles, contados a partir del día hábil siguiente del recibo de la respectiva comunicación, deberán adicionar sus comentarios y observaciones en el formulario que está disponible en el apartado *Formularios para remitir observaciones de normativa en consulta*, ubicado en la dirección electrónica de la página oficial de la Sugef:

<https://www.sugef.fi.cr/normativa/Formularios%20Normativa%20en%20Consulta.aspx>

Sin detrimento de lo anterior, las entidades consultadas pueden presentar de manera consolidada sus observaciones y comentarios a través de los gremios y cámaras que les representan. Asimismo, el correo electrónico normativaenconsulta@sugef.fi.cr será utilizado únicamente como mecanismo de notificación sobre la completitud de dicho formulario.

Proyecto de Acuerdo

“El Consejo Nacional de Supervisión del Sistema Financiero *(*Conassif).

## considerando que:

### consideraciones de orden legal y reglamentario

1. El literal b) del artículo 171 de la *Ley Reguladora del Mercado de Valores,* Ley 7732, dispone, como una de las funciones del Conassif, aprobar las normas atinentes a la autorización, regulación, supervisión, fiscalización y vigilancia que, conforme a la ley, deben ejecutar la Superintendencia General de Entidades Financieras (Sugef), la Superintendencia General de Valores (Sugeval) y la Superintendencia de Pensiones (Supen). Asimismo, el artículo 28 de la *Ley Reguladora del Mercado de Seguros,* Ley 8653, dispone, en relación con la Superintendencia General de Seguros (Sugese), que: “al superintendente y al intendente les serán aplicables las disposiciones establecidas, de manera genérica y de aplicación uniforme, para las demás Superintendencias bajo la dirección del Conassif y sus respectivos superintendentes e intendentes”.
2. El inciso d) del artículo 131 y el artículo 119 de la *Ley Orgánica del Banco Central de Costa Rica*, Ley 7558, confieren al Consejo Nacional de Supervisión del Sistema Financiero la potestad de dictar las normas generales que sean necesarias para el establecimiento de sanas prácticas bancarias de gobierno corporativo, incluidas las de idoneidad de miembros del Órgano de Dirección y puestos claves de la organización, así como de gestión de riesgos y de registro de las transacciones, entre otros aspectos, todo en salvaguarda del interés de la colectividad.
3. El inciso c) del artículo 131 de la *Ley Orgánica del Banco Central de Costa Rica*, Ley 7558, establece, como parte de las funciones del superintendente general de entidades financieras, proponer al Conassif, para su aprobación, las normas que estime necesarias para el desarrollo de las labores de supervisión y fiscalización.
4. El artículo 3 de la *Ley Reguladora del Mercado de Valores*, Ley 7732, establece que la Sugeval debe velar por la protección del inversionista y la transparencia del mercado de valores. Asimismo, el artículo 8 de la Ley 7732, 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.
5. El artículo 38, literal f) del *Régimen Privado de Pensiones*, Ley 7523, establece como una atribución del superintendente de Pensiones adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación, supervisión y fiscalización que le competen a la Superintendencia, según la ley y las normas emitidas por el Conassif.
6. Que el artículo 29 de la *Ley Reguladora del Mercado de Seguros*, Ley 8653, establece como objeto de la 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 Conassif, para su aprobación, la normativa reglamentaria que se requiera para la aplicación de esta ley, así como cumplir sus competencias y funciones.
7. El inciso n) y el sub inciso xi) del artículo 131 de la *Ley Orgánica del Banco Central de Costa Rica*, Ley 7558; el inciso r) del el artículo 38 de la *Ley de Régimen Privado de Pensiones*, Ley 7523; el inciso L) del artículo 8 de la *Ley Reguladora del Mercado de Valores*, y los incisos i) y j) del artículo 29 de la *Ley Reguladora del Mercado de Valores*, Ley 8653, facultan por su orden a la Superintendencia General de Entidades Financieras, a la Superintendencia de Pensiones, a la Superintendencia General de Valores y a la Superintendencia General de Seguros, a proponer al Conassif normas sobre el contenido, la forma y la periodicidad con que las entidades deben proporcionar a la Superintendencia, información sobre su situación jurídica, económica, financiera, de gobierno corporativo y de administración de riesgos, entre otros, para cumplir la supervisión que debe realizar cada una de las Superintendencias.
8. El inciso e) del artículo 131 de la *Ley Orgánica del Banco Central de Costa Rica*, Ley 7558; el artículo 40 de la *Ley de Régimen Privado de Pensiones*, Ley 7523; el inciso j) del artículo 8 de la *Ley Reguladora del Mercado de Valores*, y, el párrafo segundo y el inciso l) del artículo 29 de la *Ley Reguladora del Mercado de Seguros*, Ley 8653, facultan por su orden a la Superintendencia General de Entidades Financieras, a la Superintendencia de Pensiones, a la Superintendencia General de Valores y a la Superintendencia General de Seguros, a dictar medidas correctivas.
9. Mediante artículo 13 del acta de la sesión 893-2010, celebrada el 3 de diciembre del 2010, el Conassif aprobó el *Reglamento General de Auditores Externos*, Acuerdo CONASSIF 1-10, el cual regula la contratación y la prestación de los servicios de auditoría externa.
10. Mediante artículos 5 y 7, de las actas de las sesiones 1294-2016 y 1295-2016, celebradas el 8 de noviembre de 2016, el Conassif aprobó el Reglamento sobre Gobierno Corporativo, Acuerdo CONASSIF 4-16 (anteriormente conocido como Acuerdo SUGEF 16-16), mediante el cual se establecen los principios sobre gobierno corporativo que deben considerar las entidades incluidas en el alcance de ese reglamento.
11. 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, el Conassif aprobó el *Reglamento General de Gestión de la Tecnología de Información*, Acuerdo Conassif 5-17 (anteriormente conocido como Acuerdo Sugef 14-17), el cual establece los requerimientos mínimos para la gestión de la tecnología de información (TI) que deben acatar las entidades y empresas supervisadas del sistema financiero costarricense incluidas en el alcance de ese reglamento.

### consideraciones sobre la modificación integral del Reglamento General de Gestión de la Tecnología de Información

1. El Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17, requiere ser modificado integralmente con el fin de alcanzar los siguientes propósitos:
	1. Reforzar las funciones de los Órganos de Dirección, Alta Gerencia y Órganos de Control con relación al marco de gobierno y de gestión de TI, incluyendo responsabilidades sobre la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital.
	2. Actualizar el marco de gobierno y de gestión de TI e incorporar disposiciones sobre tecnologías emergentes, gobierno y gestión de la seguridad de la información; seguridad cibernética, incidentes de seguridad cibernética, tercerización de bienes y servicios de TI, computación en la nube, el tratamiento del uso y acceso de los datos y de los activos de información.

### consideraciones sobre el gobierno de la tecnología de información

1. El gobierno de la tecnología de información es una parte fundamental del gobierno corporativo y debe ser ejercido por el Órgano de Dirección, el cual, debe supervisar la definición e implementación de procesos, estructuras y mecanismos relacionados con TI. Lo anterior, con el fin de controlar eficazmente los procesos, garantizar la seguridad de la información, optimizar el uso de recursos y dar apoyo para la toma de decisiones; esto alineado con la visión, misión y objetivos estratégicos de la organización.
2. Se espera que los miembros de los Órganos de Dirección y de la Alta Gerencia se vean comprometidos a adaptar e implementar sus medidas de gobierno conforme a su contexto, necesidades específicas y riesgos.

### consideraciones prudenciales sobre la resiliencia, la continuidad de las operaciones y de los servicios de TI

1. Para hacer frente a la naturaleza cambiante de las amenazas cibernéticas, es importante que las entidades y empresas supervisadas puedan crear y mantener sistemas, herramientas tecnológicas, procesos de negocio y servicios de TI resilientes que minimicen el impacto de las amenazas. Entre otros aspectos, es importante que se pongan en marcha políticas específicas y exhaustivas de continuidad, así como diseñar planes de respuesta y recuperación para gestionar los incidentes de seguridad cibernética.

### consideraciones sobre la gestión de la tecnología de información

1. Si bien la tecnología de información es indispensable para mantener y optimizar las operaciones dentro de las organizaciones, también su uso ha ocasionado la aparición de nuevos riesgos, por lo que es importante que el marco de gobierno y de gestión de TI incluya medidas sólidas para mitigar los riesgos que genera la dependencia tecnológica de las entidades y empresas supervisadas, y así garantizar su continuidad operativa en caso de incidentes tecnológicos.
2. El diseño e implementación del marco de gestión de TI requiere de esfuerzo planificado y progresivo. Además, requiere que se considere el entendimiento de la estrategia y su contexto organizacional, la determinación del alcance y la aplicabilidad de los componentes a implementar, así como sus factores de diseño, perfilamiento del alcance, el diseño de los procesos de negocio y la dependencia tecnológica de sus actividades.

### consideraciones prudenciales sobre la seguridad de los servicios en la nube

1. La migración a la nube brinda enormes oportunidades, eficiencias y conveniencia, sin embargo, también expone a las organizaciones a una nueva gama de amenazas de seguridad cibernética.
2. Es importante que las entidades y empresas supervisadas tengan definido el modelo de responsabilidades compartidas entre el cliente (gestión propia) y el proveedor (tercerización) aplicables para cada uno de los modelos de servicios de computación en la nube, así como los controles administrativos y técnicos asociados a este tipo de servicios.

### consideraciones prudenciales sobre la tercerización de bienes y servicios de TI

1. Los proveedores de bienes y servicios son ampliamente utilizados para proporcionar servicios, sistemas y soluciones de TI que respaldan las operaciones de las organizaciones. Las vulnerabilidades de seguridad cibernética producto de la tercerización de bienes y servicios de TI podrían convertirse en canales de ciberataques, por lo que las capacidades de seguridad cibernética de los proveedores son elementos críticos.
2. Los proveedores de bienes y servicios de TI y su cadena de suministros no están dentro del alcance de esta regulación, sin embargo, es necesario que las entidades y empresas supervisadas asuman su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados; lo anterior, a través de cláusulas en los contratos y acuerdos de servicio que soliciten la inclusión de las prácticas y controles para mitigar los riesgos de tercerización de bienes y servicios de TI.
3. Los más reconocidos proveedores internacionales de servicios en la nube, servicios de cómputo, almacenamiento, bases de datos, análisis e inteligencia artificial se encuentran a la vanguardia en el uso de herramientas e implementación de políticas de seguridad cibernética, sin embargo, sus servicios suelen contratarse mediante instrumentos de adhesión; lo que hace necesario establecer un tratamiento diferenciado en la aplicación de la regulación, de manera que el marco regulatorio no impida la contratación de servicios con esos proveedores ni la supervisión por parte de las Superintendencias. En los casos en que los servicios se contraten mediante instrumentos de adhesión, la entidad debe ser responsable de asegurar la confidencialidad y la continuidad de los bienes y servicios delegados.

### consideraciones sobre la seguridad de la información y la seguridad cibernética

1. Los riesgos que amenazan la seguridad de la información y la seguridad cibernética han tomado importancia en un entorno creciente de conectividad y de dependencia de los servicios otorgados a través de plataformas tecnológicas, lo que conlleva a que las organizaciones, por una parte, deban asegurar la adecuada calidad y disponibilidad de los sistemas utilizados para la prestación de dichos servicios y , por otra parte, enfrenten una progresiva exposición a los riesgos, especialmente cuando estos se asumen en el ciberespacio.
2. Los ciberataques sufridos por entidades financieras han centrado la atención en la necesidad de reforzar la seguridad cibernética. El Consejo de Estabilidad Financiera (FSB por sus siglas en inglés) incluyó en su plan de trabajo de 2017, la necesidad de vigilar el riesgo cibernético derivado de la tecnología financiera e identificar los asuntos de supervisión y regulación desde la perspectiva de la estabilidad financiera.
3. En junio de 2016, el Comité de Pagos e Infraestructuras de Mercado (CPMI) y la Organización Internacional de Comisiones de Valores (IOSCO) publicaron orientaciones sobre la ciberresistencia de las infraestructuras de los mercados financieros. Además, en abril de 2016, la Asociación Internacional de Supervisores de Seguros (IAIS) publicó un documento temático para sensibilizar a las aseguradoras y a los supervisores sobre los retos que plantea el riesgo cibernético.
4. El Comité de Supervisión Bancaria de Basilea reconoció los beneficios de abordar la resiliencia operacional más allá del ámbito de la gestión del riesgo operacional y los requerimientos de capital mínimos. A principios de 2018, estableció el grupo de trabajo de resiliencia operacional (ORG) con la intención de contribuir, entre otros aspectos, a los esfuerzos internacionales relacionados con la gestión del riesgo cibernético.
5. Es importante que las entidades y empresas supervisadas cuenten con un marco regulatorio que contemple las buenas prácticas en materia de seguridad cibernética, lo que deriva en mejoras para contar con una adecuada gestión de su negocio, así como anticiparse a posibles escenarios adversos. El presente reglamento otorgará claridad a las entidades y entidades supervisadas sobre los elementos mínimos de seguridad de la información y seguridad cibernética que resultan esenciales para el regulador, así como la notificación oportuna de incidentes, sus impactos y su gestión.
6. Se espera que las entidades y empresas supervisadas establezcan un Sistema de Gestión de Seguridad de la Información a través de la definición de estructuras generales para el gobierno y gestión, de conformidad con lo establecido en el marco de gestión de TI del presente reglamento.

### consideraciones prudenciales sobre la auditoría externa de TI

1. El proceso de supervisión de TI se apoya en auditorías externas especializadas, cuyos alcances son definidos por el supervisor a partir de un conjunto de procesos de evaluación relacionados con el marco de gobierno y de gestión de TI, en congruencia con el perfil tecnológico comunicado por las entidades y empresas supervisadas.
2. La auditoría de TI es una actividad especializada para la cual existen certificaciones con reconocimiento mundial. En el caso de la certificación Certified Information Systems Auditor (CISA por sus siglas en inglés), esta reconoce las aptitudes y conocimientos de un profesional en las áreas de auditoría de sistemas de información, gobierno y mantenimiento de TI, adquisición, desarrollo e implementación de sistemas de información, operaciones, mantenimiento y soporte de sistemas de información y protección de activos de información.

### consideraciones sobre los estándares internacionales, mejores prácticas y marcos de referencia

1. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de Costa Rica estableció una Estrategia Nacional de Ciberseguridad con el objetivo de diseñar un marco para orientar las acciones que el país puede tomar con respecto al uso seguro de TI y desarrollar la coordinación y cooperación entre las partes interesadas. El papel del regulador incluye contar con un marco normativo basado en buenas prácticas para la protección de infraestructuras críticas con el fin de desarrollar una infraestructura de monitoreo y alerta temprana para la detección, prevención y respuesta de incidentes de seguridad cibernética.
2. La industria y los profesionales en TI han desarrollado estándares, buenas prácticas y marcos de referencia para gestionar y controlar las tecnologías y sus riesgos relacionados, los cuales han sido considerados en las disposiciones del presente reglamento y estos, a su vez, se alinean con el objetivo de la Estrategia Nacional de Ciberseguridad establecida por el MICITT.
3. El marco de referencia COBIT 2019 permite la alineación, interoperabilidad e integración con los estándares, buenas prácticas y otros marcos de referencia desarrollados por la industria y los profesionales de TI, lo cual permite fortalecer el control interno de las tecnologías de información.
4. En la industria de TI, se identifican un conjunto de marcos de referencia y estándares en materia de seguridad cibernética, como el caso de los estándares desarrollados por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés), que se enfocan en el uso de impulsores de negocios para guiar las actividades de seguridad cibernética y en la consideración de los riesgos de seguridad cibernética. Asimismo, se desarrollaron las normas ISO que disponen de estándares orientados en materia de seguridad cibernética y los Controles CIS del Center for Internet Security.
5. La regulación permite que las entidades y empresas supervisadas utilicen los estándares internacionales, mejores prácticas y marcos de referencia que la industria de tecnologías ha desarrollado para la implementación del marco de gobierno y de gestión de TI, sin perjuicio del cumplimiento de las disposiciones establecidas en este reglamento.

### consideraciones de costo-beneficio

1. La evaluación costo-beneficio de la regulación se realiza de conformidad con lo establecido en los artículos 1 y 12 de la Ley Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, Ley 8220 y en los artículos 12, 12 bis, 13, 13 bis y 56 al 60 bis del Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, 37045-MP-MEIC. Dicha regulación indica que la Administración Pública debe realizar un análisis de impacto regulatorio mediante una evaluación costo-beneficio antes de emitir cualquier nueva regulación o reformar las existentes, cuando establezcan trámites, requisitos y procedimientos que deba cumplir el administrado ante la Administración. De dicho análisis se determinó que la regulación no establece ni modifica trámites, requisitos o procedimientos que el administrado deba cumplir ante la Administración Central.

### otras consideraciones

1. El presente reglamento está alineado a los marcos regulatorios transversales y específicos aprobados por el CONASSIF, relacionados con la supervisión basada en riesgos, supervisión consolidada, gobierno corporativo, la gestión integral de riesgos, las auditorías externas, así como la calificación de entidades y empresas supervisadas establecidas por cada Superintendencia.

**dispuso:**

modificar integralmente el Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17, de conformidad con el texto que se incluye a continuación:

# **‘REGLAMENTO GENERAL DE GOBIERNO Y GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN**

**ACUERDO CONASSIF 5-24**

## CAPÍTULO I

## DISPOSICIONES GENERALES

#### ***Artículo 1. Objeto***

*Este reglamento tiene como finalidad establecer los requerimientos para el gobierno y la gestión de la tecnología de información y sus riesgos asociados, que deben ser acatados por las entidades y empresas supervisadas del sistema financiero costarricense.*

*La presente regulación se tendrá como plenamente integrada y complementaria al marco general de gobierno y de gestión de riesgos establecido en el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16 y en el marco de regulación vigente sobre gestión de riesgos de cada Superintendencia.*

#### ***Artículo 2. Alcance***

*Las disposiciones establecidas en este reglamento son de aplicación para:*

1. Supervisados por SUGEF:
2. *Bancos comerciales del Estado*
3. *Bancos creados por ley especial*
4. *Bancos privados*
5. *Empresas financieras no bancarias*
6. *Organizaciones cooperativas de ahorro y crédito*
7. *Mutuales de ahorro y préstamo*
8. *Caja de Ahorro y Préstamos de la ANDE*
9. Supervisados por SUGEVAL:
10. *Puestos de bolsa y sociedades administradoras de fondos de inversión*
11. *Bolsas de valores*
12. *Sociedades de compensación y liquidación*
13. *Proveedores de precio*
14. *Entidades que brindan servicios de custodia*
15. *Centrales de valores*
16. *Sociedades titularizadoras y fiduciarias*
17. *Entidades de registros centralizados de letras de cambio y pagarés electrónicos*
18. Supervisados por SUGESE:
19. *Entidades aseguradoras y reaseguradoras*
20. *Sucursales de entidades aseguradoras extranjeras*
21. *Sociedades corredoras de seguros*
22. Supervisados por SUPEN:
23. *Operadoras de pensiones complementarias*
24. *Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social.*
25. *Fondos complementarios creados por leyes especiales o convenciones colectivas*

*Tratándose del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense del Seguro Social, las disposiciones y lineamientos incorporados en este reglamento tienen el carácter de adopción y aplicación voluntaria.*

*Se exceptúan del alcance del presente reglamento a 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 que son administrados por una operadora de pensiones o en los casos en que la unidad de TI y su gestión de TI es regulada por una norma de tecnología de información de alcance general, cuyo cumplimiento esté debidamente fiscalizado, así como los fondos de pensiones cerrados a nuevas afiliaciones.*

1. Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados.

#### ***Artículo 3. Regulación Proporcional***

*La aplicación proporcional y diferenciada del presente reglamento para las entidades supervisadas por SUGEF sujetas a la Regulación proporcional para cooperativas de ahorro y crédito, Acuerdo SUGEF 25-23 y para las sociedades corredoras de seguros supervisadas por SUGESE será la siguiente:*

1. *Lo dispuesto en los capítulos que se indican a continuación se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades:*
2. Capítulo II Gobierno y Gestión de TI.
3. Capítulo III Organización de las tecnologías de información.
4. *Lo dispuesto en el Capítulo IV Seguridad de la información y seguridad cibernética, será de aplicación plena, salvo en el caso de lo dispuesto en el artículo 33. Programas de análisis de vulnerabilidades y pruebas, en el artículo 34.Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de seguridad cibernética y en el artículo 35.Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética, del presente reglamento.*
5. *Lo dispuesto en el Capítulo V La auditoría externa de TI, será de aplicación plena, salvo lo dispuesto en el artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI, en el artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética y en el inciso b) del artículo 47. Alcance y plazo de la Auditoría Externa de TI. Además, deben considerarse los aspectos siguientes:*
6. Las entidades, en función de su perfil de riesgo y de la naturaleza de sus operaciones, definirán el alcance de la auditoría externa estableciendo los procesos de evaluación que consideren pertinentes, según el anexo 1 de los lineamientos generales del presente reglamento. Sin perjuicio de lo anterior, el alcance de la auditoría externa deberá incluir, al menos, los procesos de evaluación que se especifican en el anexo 2 de los lineamientos generales del presente reglamento.
7. La solicitud de la auditoría externa será cada tres años, excepto cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de anticiparla o aplazarla.

#### ***Artículo 4. Definiciones y abreviaturas***

*Para efectos de este reglamento y sus lineamientos generales, se utilizan las siguientes definiciones y abreviaturas:*

1. **Bienes y servicios de TI críticos:** Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación.
2. **Declaración de aplicabilidad:** Documento que permite identificar y revelar los controles de seguridad de la información y de la seguridad cibernética elegidos por la entidad o empresa supervisada para proteger sus activos de información, basándose en la evaluación de riesgos.
3. **Gestión de TI:** Estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la tecnología de la información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.
4. **ISACA:** Acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association).
5. **Marco de gestión de TI:** Conjunto de procesos destinados a gestionar las tecnologías de información de las entidades y empresas supervisadas, 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 estas tienen en los procesos de TI.
6. **Perfil tecnológico:** Descripción de la estructura de gobierno y gestión, los procesos, servicios, infraestructura de TI, proveedores de bienes y servicios de TI, inventario de tipos documentales, proyectos de TI, planes de adquisición y gestión de riesgos de TI.
7. **Plan de acción:** Conjunto de acciones, plazos y responsables enfocados en atender los hallazgos y riesgos detectados en el informe de auditoría y comunicados en el reporte de supervisión.
8. **Procesos críticos:** Son aquellos procesos que tienen un impacto significativo en la consecución de los objetivos estratégicos previstos por la entidad o empresa supervisada. Estos procesos están relacionados con la naturaleza, misión, objetivos y función de la entidad o empresa supervisada y son indispensables para la continuidad del negocio y de sus operaciones.
9. **Proveedores de bienes y servicios de TI críticos:** Persona física o jurídica que provee bienes o servicios relacionados con TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).
10. **Resiliencia operativa digital:** Capacidad de una entidad o empresa supervisada para mantener la continuidad y la disponibilidad de sus operaciones digitales y tecnológicas incluso en situaciones adversas. Implica la implementación de medidas proactivas y estrategias para garantizar que las operaciones digitales sigan funcionando de manera eficiente y segura, minimizando el impacto de los incidentes.
11. **Seguridad cibernética:** Práctica de proteger sistemas, redes, dispositivos y datos digitales contra amenazas, ataques y actividades maliciosas en el ciberespacio, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información y de los recursos digitales.
12. **Tecnología de información (TI):** 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.
13. **Unidad de TI o función equivalente:** Instanciao función que provee los procesos y servicios de TI para las entidades y empresas supervisadas.

*Este reglamento incorpora como propias las demás definiciones dispuestas en la reglamentación vigente aprobada por el CONASSIF.*

#### ***Artículo 5. Lineamientos generales***

*Los superintendentes podrán emitir, conjuntamente, los lineamientos generales que consideren necesarios para la aplicación de este reglamento.*

## CAPÍTULO II

## GOBIERNO Y GESTIÓN DE TI

### *Sección I. Marco de gobierno y gestión de TI*

#### ***Artículo 6. Marco de gobierno y gestión de TI***

*Las entidades y empresas supervisadas deben diseñar, implementar, controlar y mantener un marco de gobierno y gestión de TI de conformidad con la estrategia organizacional, el apetito de riesgo, el nivel de tolerancia al riesgo y las políticas aprobadas por el Órgano de Dirección.*

*Asimismo, las entidades y empresas supervisadas podrán utilizar los estándares internacionales, mejores prácticas y marcos de referencia que la industria de tecnologías ha desarrollado para la implementación del marco de gobierno y gestión de TI, sin perjuicio del cumplimiento de las disposiciones establecidas en este reglamento.*

***Artículo 7. Propósitos del marco de gobierno y gestión de TI***

*El marco de gobierno y gestión de TI debe permitir a las entidades y empresas supervisadas cumplir con los siguientes propósitos:*

1. Orientar hacia la definición del gobierno de TI con un enfoque integrado y alineado con el gobierno corporativo.
2. Asegurar un equilibrio entre el uso de los recursos de TI y los procesos críticos de negocio.
3. Crear valor mediante los beneficios de las tecnologías de información, dentro de los márgenes de apetito al riesgo.
4. Asegurar que la planificación y el desarrollo de TI se realice de conformidad con lo definido por la entidad o empresa supervisada, de tal forma que se garantice que TI contribuye en satisfacer las necesidades y expectativas organizacionales.
5. Establecer una dirección estratégica sólida y una estructura eficiente para gestionar TI; asimismo, alinear los objetivos de la entidad o empresa supervisada con el uso de la tecnología y su arquitectura organizacional.
6. Implementar la planificación estratégica, así como la gestión de la innovación y de la arquitectura organizacional.
7. Gestionar el presupuesto, los costos, el conocimiento y el recurso humano de las unidades de TI, así como las relaciones con las partes interesadas.
8. Establecer la gestión de los acuerdos de nivel de servicio, de los proveedores de bienes y servicios de TI y de los riesgos de TI. Además del diseño e implementación de sistemas integrados de calidad y de seguridad de la información, así como la gestión de activos de información y de los datos.
9. Definir la gestión del portafolio y de los programas y proyectos de TI que permitan atender la definición de los requisitos del negocio, según corresponda.
10. Determinar la estrategia de adquisición, construcción e implementación de soluciones tecnológicas integradas al negocio.
11. Gestionar la disponibilidad y la capacidad de infraestructura tecnológica y asegurar la continuidad de las operaciones.
12. Asegurar la configuración de los activos de información, considerando la gestión, aceptación y transición de los cambios.
13. Gestionar las operaciones de TI, los incidentes de los bienes y servicios, además, la solución de los problemas de TI, los servicios de seguridad de la información y de seguridad cibernética, los controles de los procesos del negocio, así como asegurar una resiliencia operativa digital.
14. Gestionar el monitoreo del desempeño y la conformidad de los procesos, el sistema de control interno, el cumplimiento de los requisitos externos y el aseguramiento de TI.

### *Sección II. Responsabilidades del Órgano de Dirección*

***Artículo 8. Responsabilidades generales sobre el gobierno de TI***

*En relación con el gobierno de TI, el Órgano de Dirección, al menos, debe:*

1. Aprobar el marco de gobierno y gestión de TI y el apetito de sus riesgos asociados.
2. Establecer un Comité de TI o una función equivalente y aprobar sus normas de gobierno y gestión.
3. Designar la firma de auditoría externa o el profesional independiente de TI que realizará las auditorías solicitadas por las Superintendencias.
4. Aprobar las políticas, estructuras, planes estratégicos, recursos, inversiones y presupuestos necesarios para la implementación del marco de gobierno y gestión de TI, incluyendo tecnologías emergentes.
5. Aprobar los informes de la auditoría externa de TI que serán remitidos a las Superintendencias.
6. Aprobar los planes de acción para la atención de los hallazgos y de los riesgos que se identifiquen como resultado de la auditoría externa de TI.
7. Evaluar las necesidades de las partes interesadas para lograr un equilibrio entre los objetivos del negocio y los objetivos de TI definidos por la entidad o empresa supervisada.
8. Asegurar que se resguarde la confidencialidad e integridad de los datos y de la información crítica de las partes interesadas y de la entidad o empresa supervisada que sea utilizada por los proveedores.

***Artículo 9. Responsabilidades sobre la seguridad de la información y la seguridad cibernética***

*En relación con el gobierno de la seguridad de la información y de la seguridad cibernética, el Órgano de Dirección, al menos, debe:*

1. Asegurar que la gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética estén integrados dentro de la gestión de riesgos de la entidad o empresa supervisada.
2. Asignar tiempo a las discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética en las reuniones del Órgano de Dirección.
3. Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles.
4. Asegurar que se apliquen medidas para la atención de los incidentes de seguridad de la información y de seguridad cibernética.
5. Aprobar los planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética.
6. Asegurar que los requerimientos de seguridad de la información y de seguridad cibernética de la entidad o empresa supervisada sean de cumplimiento por parte de los proveedores de bienes y servicios de TI.

***Artículo 10. Responsabilidades sobre la resiliencia operativa digital***

*En relación con el gobierno de la resiliencia operativa digital, el Órgano de Dirección, al menos, debe:*

1. Asegurar la resiliencia operativa digital para la continuidad de las operaciones de la entidad o empresa supervisada.
2. Establecer y aprobar la estrategia de la resiliencia operativa digital.
3. Aprobar los presupuestos y recursos necesarios para la implementación de la estrategia de resiliencia operativa digital.
4. Asegurar que se implementen planes de respuesta, recuperación y atención de crisis para gestionar los incidentes de seguridad cibernética que podrían interrumpir la ejecución de los procesos críticos.
5. Asegurar que los planes de respuesta de incidentes de seguridad cibernética sean acordes con el apetito de riesgo y la tolerancia establecida por la entidad o empresa supervisada.

### *Sección III. Responsabilidades de la Alta Gerencia y del Comité de TI o de la función equivalente*

#### ***Artículo 11. Responsabilidades de la Alta Gerencia sobre el gobierno y la gestión de TI***

*En relación con el gobierno y la gestión de TI, la Alta Gerencia, al menos, debe:*

1. Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección.
2. Proponer al Órgano de Dirección las estrategias y los recursos requeridos para la implementación del marco de gobierno y gestión de TI.
3. Implementar las políticas relacionadas con TI aprobadas por el Órgano de Dirección.
4. Designar las áreas de negocio y de TI responsables de implementar el marco de gobierno y de gestión TI.
5. Implementar los planes de acción para la atención de los hallazgos de la auditoría externa de TI.

#### ***Artículo 12. Comité de TI o función equivalente***

*Las entidades y empresas supervisadas deben contar con un Comité de TI o función equivalente, el cual responderá al Órgano de Dirección en sus funciones.*

*Los grupos y conglomerados financieros pueden contar con un Comité de TI corporativo o funciones equivalentes a nivel corporativo, en cuyo caso se podrá coordinar, aplicar y mantener un único marco de gobierno y gestión de TI.* *Las condiciones para tipificar un Comité de TI como corporativo están establecidas en los lineamientos generales del presente reglamento.*

*La designación de los integrantes del Comité de TI corporativo la determinará el propio grupo o conglomerado financiero y deberá asegurarse la representación de las entidades y empresas que lo integran, así como un balance entre conocimiento del negocio y de TI.*

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

#### ***Artículo 13. Responsabilidades del Comité de TI o de la función equivalente***

*Corresponden al Comité de TI o a la función equivalente, al menos, las siguientes responsabilidades:*

1. Supervisar la implementación del marco de gobierno y gestión de TI.
2. Asesorar al Órgano de Dirección y a la Alta Gerencia en la formulación de las estrategias y las metas de TI; asimismo, velar por su cumplimiento.
3. Proponer al Órgano de Dirección las políticas relacionadas con TI.
4. Proponer al Órgano de Dirección los planes de acción que, cuando corresponda, atenderán las observaciones incluidas en el reporte de supervisión de TI, así como monitorear su implementación.
5. Aprobar los procedimientos, los instructivos y la documentación operativa de TI.
6. Recomendar al Órgano de Dirección las prioridades para las inversiones en TI.
7. Validar que la firma de auditores externos o el profesional independiente de TI tengan los conocimientos y la experiencia para auditar aspectos de seguridad de la información, seguridad cibernética y tecnologías emergentes, de conformidad con el alcance solicitado.
8. Validar el estudio técnico en el que se fundamentan los procesos de evaluación del marco de gobierno y gestión de TI que no le aplican a la entidad o empresa supervisada.

### *Sección IV. Responsabilidades de los Órganos de Control*

#### ***Artículo 14. Responsabilidades sobre la Auditoría Interna o de la función equivalente***

*En relación con las tecnologías de información, la Auditoría Interna o la función equivalente, al menos, debe:*

1. Supervisar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.
2. Implementar un plan de auditoría basado en el riesgo para evaluar la calidad y la eficacia del marco de gobierno y gestión de TI, de la seguridad de la información y de la seguridad cibernética.
3. Evaluar la calidad y eficacia de los planes de acción elaborados por la entidad o empresa supervisada que, cuando correspondan, atenderán los hallazgos que se identifiquen como resultado de la auditoría externa de TI.
4. Ejecutar trabajos específicos requeridos por las Superintendencias.

#### ***Artículo 15. Responsabilidades de la unidad o función de gestión de riesgos***

*En relación con las tecnologías de información, la unidad o función de gestión de riesgos, al menos, debe:*

1. Incorporar la gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética dentro de la gestión de riesgos de la entidad o empresa supervisada.
2. Incorporar el apetito de riesgo y la tolerancia de los riesgos tecnológicos, de seguridad de la información y de seguridad cibernética, dentro de la declaración de apetito de riesgo de la entidad o empresa supervisada.
3. Ejecutar trabajos específicos requeridos por las Superintendencias.

## CAPÍTULO III

## ORGANIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

### *Sección I. Generalidades de la gestión de TI*

#### ***Artículo 16. Gestión de TI individual o función corporativa***

*La gestión de TI de las entidades y empresas supervisadas es tipificada de manera predeterminada como gestión de TI individual.*

*Los grupos y conglomerados financieros pueden solicitar al supervisor responsable, un permiso para tipificar su gestión de TI como corporativa, en cuyo caso, se podrá coordinar, aplicar y mantener un único marco de gobierno y de gestión de TI, el cual debe contemplar los riesgos de TI establecidos en la declaración de apetito de riesgo aprobada por el Órgano de Dirección para cada una de las entidades y empresas supervisadas.*

*La solicitud debe contener una justificación debidamente sustentada que demuestre que se cumplen las condiciones para que la gestión de TI sea tipificada como corporativa. Las condiciones para tipificar la gestión de TI como corporativa están establecidos en los lineamientos generales del presente reglamento, así como el plazo de respuesta. Las Superintendencias deben coordinar la respuesta a esta solicitud.*

*En el caso que se determine que la gestión de TI corporativa no atiende en forma adecuada y oportuna las funciones y obligaciones indicadas en este reglamento, para alguna de las entidades o empresas que constituyen el grupo o conglomerado, la Superintendencia responsable de la supervisión de dicha entidad o empresa puede requerir que se establezca una gestión de TI individual para la respectiva entidad o empresa.*

*El proceso de intercambio de información entre Superintendencias se hará en los términos dispuestos en Reglamento sobre procedimiento de intercambio de información entre las Superintendencias del sistema financiero, Acuerdo CONASSIF 7-19.*

#### ***Artículo 17. Unidad de TI o función equivalente***

*Las entidades y empresas supervisadas deben establecer una Unidad de TI o una función equivalente encargada de implementar y desarrollar soluciones tecnológicas para apoyar y facilitar la ejecución de los procesos internos, así como su marco de gobierno y gestión de TI.*

#### ***Artículo 18. Responsabilidades de la unidad de TI o de la función equivalente***

*La Unidad de TI o la función equivalente es responsable de:*

1. Ejecutar las acciones del marco de gobierno y gestión de TI que le correspondan a la entidad o empresa supervisada.
2. Gestionar los riesgos tecnológicos de conformidad con el apetito y la tolerancia del riesgo de la entidad o empresa supervisada.
3. Desarrollar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada.
4. Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos acordados.
5. Asegurar que la gestión de los datos de la entidad o empresa supervisada se realice de manera efectiva y eficiente, atendiendo, en función de sus riesgos, las necesidades de confidencialidad, integridad, disponibilidad, no repudio y auditabilidad.
6. Diseñar un modelo de arquitectura para soportar las operaciones de la entidad o empresa supervisada.
7. Establecer los controles para el desarrollo del ciclo de vida de los servicios y de los sistemas de información, los cuales aseguren la confidencialidad, integridad, disponibilidad, calidad, mantenimiento y los cambios por excepción o de emergencia.
8. Verificar el cumplimiento contractual por parte de los proveedores cuando se les delegan bienes o servicios de TI.
9. Asegurar que los bienes y servicios de TI críticos estén identificados, sean gestionados de manera efectiva y eficiente, y se mantengan disponibles.
10. Asegurar que los requerimientos de las entidades y empresas supervisadas sean atendidos de manera equitativa y en función de los riesgos de cada negocio cuando la gestión de TI es corporativa.

### *Sección II. Tratamiento de datos, activos de información, aplicaciones, sistemas de información y soluciones tecnológicas*

***Artículo 19. Clasificación de activos de información, del impacto en caso de presentarse una brecha de seguridad de la información y del acceso y uso de los datos***

*Las entidades y empresas supervisadas deben* *clasificar sus activos de información, el impacto potencial en caso de presentarse una brecha de seguridad de la información, así como el acceso y uso de los datos y los activos de información de conformidad con el modelo de clasificación establecido en los lineamientos generales del presente reglamento.*

*Los activos de información primarios y de apoyo deben ser revelados en el perfil tecnológico.*

#### ***Artículo 20. Bases de datos, aplicaciones, sistemas de información y soluciones tecnológicas***

#### *Las bases de datos actualizadas, las aplicaciones, los sistemas de información y las soluciones tecnológicas vigentes que procesan o dan acceso a las bases de datos de las entidades o empresas supervisadas deben estar disponibles y accesibles a las Superintendencias para sus labores de supervisión, sin ningún tipo de restricción o condición.*

*Cuando existan bases de datos compartidas debe efectuarse una separación del registro de las operaciones de cada entidad y empresa integrante del grupo o conglomerado financiero. Asimismo, la plataforma tecnológica donde se procesen estas bases de datos solo puede ser utilizada por las entidades y empresas integrantes del grupo o conglomerado financiero.*

*Las bases de datos, las aplicaciones, los sistemas de información y las soluciones tecnológicas deben estar declarados en el perfil tecnológico.*

#### ***Artículo 21. Gestión de aplicaciones, sistemas de información y soluciones tecnológicas seguras***

*Las entidades y empresas supervisadas deben gestionar aplicaciones, sistemas de información y soluciones tecnológicas seguras mediante el establecimiento de controles relacionados con la adquisición o el desarrollo del ciclo de vida del software y la codificación segura.*

*Las pautas para la implementación de los controles están establecidas en los lineamientos generales del presente reglamento.*

### *Sección III. Gestión de la computación en la nube*

***Artículo 22. Servicios de computación en la nube***

*Las entidades y empresas supervisadas pueden disponer de sus componentes tecnológicos mediante el uso de servicios de computación en la nube, siempre y cuando, cumplan con las obligaciones generales para uso de la computación en la nube establecidas en el presente reglamento.*

*Cuando las entidades y empresas supervisadas deleguen sus procesos críticos a través de servicios de computación en la nube, deben establecer el modelo de responsabilidades compartidas para proteger la infraestructura en la que se ejecutan los servicios que se ofrecen en la nube.*

*Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando:*

1. no se cumplan los requisitos legales y de seguridad;
2. no se brinde acceso al supervisor, o
3. la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética.

***Artículo 23. Obligaciones generales para el uso de la computación en la nube***

*Las entidades y empresas supervisadas que utilicen servicios de computación en la nube deben:*

1. Gestionar los riesgos derivados del uso de servicios de computación en la nube.
2. Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube, considerando la seguridad, fiabilidad, escalabilidad, costo, soporte, experiencia, interoperabilidad y cumplimiento regulatorio.
3. Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001 y cumpla con estándares o buenas prácticas, tales como las ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (System and Organization Controls por sus siglas en inglés) SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares.
4. Verificar que, para los servicios de computación en la nube de los modelos de infraestructura como servicio (IaaS por sus siglas en inglés) y de plataforma como servicio (PaaS por sus siglas en inglés), el proveedor ofrezca un nivel TIER III o superior. Para el modelo de software como un servicio (SaaS por sus siglas en inglés), el nivel debe ser, al menos, TIER II.
5. Establecer controles para asegurar la disponibilidad acordada del servicio con el proveedor.
6. Establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe estar a disposición de la entidad o empresa supervisada en un sitio alterno que asegure la confidencialidad, integridad y disponibilidad de la información.
7. Mantener cifrada la información, cuyo uso o acceso esté clasificado como confidencial, ya sea en tránsito o en reposo, mediante el empleo de estándares y algoritmos reconocidos internacionalmente.
8. Tener bajo su control la administración de usuarios y privilegios para el acceso a los servicios de computación en la nube, a las plataformas, las aplicaciones y las bases de datos que operen en la nube; lo anterior, de conformidad con el modelo de servicio contratado.
9. Contar con sistemas de registro, monitoreo y alarma de eventos de incidentes de seguridad de la información y seguridad cibernética.
10. Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente.
11. Monitorear el cumplimiento de los acuerdos de niveles de servicio establecidos con el proveedor de servicios en la nube y, en caso de que aplique, de sus subcontratistas.
12. Contar con canales de comunicación con el proveedor de servicios en la nube, cifrados de extremo a extremo, y que, en lo posible, utilicen diferentes rutas.

***Artículo 24. Documentación de los servicios de computación en la nube***

*Las entidades y empresas supervisadas deben mantener actualizada y a disposición de las Superintendencias la documentación de los servicios de computación en la nube relacionada con:*

1. Los procesos, los servicios, los procedimientos y las aplicaciones que se ejecutan en la nube.
2. Los flujos de datos de los procesos críticos del negocio que utilizan los servicios de computación en la nube.
3. Diagramas de red que permitan identificar la plataforma que soporta el servicio de computación en la nube contratado.
4. Procedimientos para verificar el cumplimiento de los acuerdos y de los niveles de servicio establecidos con el proveedor.
5. Informes de auditoría, pruebas de seguridad en la nube y estado actual de los servicios contratados, los cuales deben actualizarse anualmente.
6. Informes de riesgos actualizados, al menos, anualmente o cuando se presenten variaciones en los servicios.
7. Informes anuales de monitoreo de servicios.
8. Modelo de seguridad establecido para el servicio de computación en la nube.
9. Contratos y acuerdos de niveles de servicios establecidos con el proveedor de los servicios de computación en la nube.

### *Sección IV. Tercerización de bienes y servicios de TI*

***Artículo 25. Responsabilidades sobre la tercerización de la información y de los bienes y servicios de TI***

*Las entidades y empresas supervisadas son responsables del gobierno, la gestión, la seguridad de la información y la seguridad cibernética de los bienes y servicios de TI que les son suministrados por terceros. Para estos efectos, se entiende por terceros: proveedores, alianzas estratégicas, negocios conjuntos, convenios u otro tipo de arreglo comercial.*

*Lo anterior incluye a entidades y empresas integrantes de grupos y conglomerados financieros supervisados, o entidades y empresas del grupo económico.*

*Se deben establecer controles a fin de comprobar que los proveedores implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los requerimientos de la entidades y empresas supervisadas.*

*Cuando los bienes y servicios de TI críticos sean proveídos por terceros, las entidades y empresas supervisadas deben asegurar que, en caso de que estos sean subcontratados, se cuente con controles de seguridad y planes de continuidad del negocio.*

***Artículo 26. Identificación de bienes y servicios de TI proveídos por terceros***

*Las entidades y empresas supervisadas deben establecer procedimientos que permitan mantener identificados los bienes y servicios de TI proveídos por terceros. Además, deben mantener identificados sus proveedores de bienes y servicios de TI críticos, a través de un análisis de riesgos.*

***Artículo 27. Identificación, evaluación y monitoreo de los riesgos de tercerización de bienes y servicios de TI críticos***

*Las entidades y empresas supervisadas deben identificar, evaluar y monitorear, de conformidad con las políticas establecidas, los riesgos de tercerización de bienes y servicios de TI críticos, así como revelar dichos riesgos en el perfil tecnológico.*

***Artículo 28. Acuerdos de confidencialidad***

*Las entidades y empresas supervisadas que deleguen bienes y servicios de TI a terceros deben suscribir acuerdos de confidencialidad previo al intercambio de información con los proveedores.*

*Las entidades y empresas supervisadas deben asegurar la confidencialidad de la información incluso en los casos en que se celebren contratos de adhesión con los proveedores.*

***Artículo 29. Contratos y acuerdos de nivel de servicio***

*Las entidades y empresas supervisadas deben establecer procesos para gestionar los contratos y los acuerdos de nivel de servicio que se celebren con sus proveedores de bienes y servicios de TI.*

*Los contratos y acuerdos de nivel de servicio deben contener cláusulas que aseguren la continuidad de los bienes y servicios de TI tercerizados.*

*Los elementos que se deben considerar para el diseño de los contratos y acuerdos de nivel de servicio están establecidos en los lineamientos generales del presente reglamento.*

*Las entidades y empresas supervisadas deben asegurar la continuidad de los bienes y servicios tercerizados incluso en los casos en que se celebren contratos de adhesión con los proveedores.*

***Artículo 30. Acceso de las Superintendencias a la información***

*Las entidades y empresas supervisadas deben asegurar, a través de los contratos y los acuerdos de nivel de servicio, que las Superintendencias tengan acceso a los registros, datos e información de los bienes y servicios de TI tercerizados.*

*Las entidades y empresas supervisadas deben asegurar el acceso de las Superintendencias a los registros, datos e información de los bienes y servicios tercerizados incluso en los casos en que se celebren contratos de adhesión con los proveedores.*

## CAPÍTULO IV

## SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD CIBERNÉTICA

### *Sección I. Gestión de la seguridad de la información y la seguridad cibernética*

***Artículo 31. Sistema de gestión de la seguridad de la información***

*Las entidades y empresas supervisadas deben diseñar, implementar, mantener y monitorear un sistema de gestión de la seguridad de la información que incluya las disposiciones de seguridad cibernética del presente reglamento.*

*El sistema de gestión de la seguridad de la información debe establecer los controles que permitan adoptar un enfoque basado en el riesgo, para proteger los activos de información y los activos que soportan la información, contra los riesgos de la seguridad de la información y la seguridad cibernética.* *Los controles deberán ser revelados mediante una declaración de aplicabilidad y especificar los atributos que están establecidos en los lineamientos generales del presente reglamento.*

*Para la implementación del sistema de gestión de la seguridad de la información, se pueden utilizar los estándares internacionales, mejores prácticas o marcos de referencia relacionados con la seguridad de la información y la seguridad cibernética que la industria de tecnologías ha desarrollado.*

*Las Superintendencias podrán requerir la inclusión de prácticas y controles de seguridad de la información y seguridad cibernética dentro del sistema de gestión de la seguridad de la información de acuerdo con las necesidades de supervisión y el riesgo identificado.*

***Artículo 32. Seguridad cibernética***

*Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital. Además, deben establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.*

*En caso de que la seguridad cibernética esté integrada, los controles deben estar identificados. Si está separada, se deben diseñar, implementar y monitorear los principios, políticas y procedimientos, así como establecer los presupuestos, las tecnologías, la formación y el recurso humano necesarios para gestionar el riesgo de la seguridad cibernética.*

*Las entidades y empresas supervisadas deben establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética.*

***Artículo 33. Programas de análisis de vulnerabilidades y pruebas***

*Las entidades y empresas supervisadas deben establecer, anualmente, programas de análisis de vulnerabilidades y pruebas que incluyan los controles de seguridad de la información y seguridad cibernética.*

*Los análisis de vulnerabilidades, así como los tipos de pruebas y sus alcances, deben ser acordes con los riesgos de seguridad de la información y seguridad cibernética de las entidades y empresas supervisadas.*

*Los análisis de las vulnerabilidades y las pruebas pueden ser ejecutados por personal interno, personal externo o ambos.*

***Artículo 34. Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de seguridad cibernética***

*Las entidades y empresas supervisadas deben establecer unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen los riesgos de la seguridad cibernética.*

*Las unidades, funciones organizacionales, centros de operaciones o comités técnicos deben establecerse de conformidad con la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por las entidades o empresas supervisadas. Además, pueden estar integrados a las áreas o funciones de seguridad de la información de las entidades o empresas supervisadas, tercerizadas o separadas.*

*En todo caso, deben establecerse las políticas y los procedimientos que definan los propósitos, responsabilidades, actividades y controles requeridos para su operación.*

***Artículo 35. Planes de promoción de la cultura de la seguridad de la información y la seguridad cibernética***

*Las entidades y empresas supervisadas deben diseñar e implementar, anualmente, planes de promoción de la cultura de la seguridad de la información y la seguridad cibernética.*

*Los planes deben incluir, al menos, actividades de capacitación, concientización, divulgación, comunicación y promoción de una cultura organizacional de seguridad de la información y seguridad cibernética dirigidos a sus colaboradores, clientes, proveedores y demás partes interesadas.*

*Los planes deben contener indicadores de medición para determinar el nivel de concientización de las entidades o empresas supervisadas.*

### *Sección II. Incidentes de seguridad cibernética*

***Artículo 36. Gestión de incidentes de seguridad cibernética***

*Las entidades y empresas supervisadas deben diseñar e implementar un proceso para la gestión de incidentes de seguridad cibernética que incorpore las fases de la gestión de incidentes establecidas en los lineamientos generales del presente reglamento.*

*El proceso de gestión de incidentes debe establecer un plan de respuesta a incidentes de seguridad cibernética y los controles a fin de recopilar las evidencias para el análisis forense durante la gestión del incidente.*

***Artículo 37. Función de respuesta a incidentes de seguridad cibernética***

*Las entidades y empresas supervisadas deben establecer una función de respuesta a incidentes de seguridad cibernética, de conformidad con su estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados.*

*La función de respuesta a incidentes de seguridad cibernética puede estar conformada por personal de diferentes áreas de la entidad o empresa supervisada, o cualquier otro miembro que se considere necesario.*

*Las principales actividades de la función de respuesta a incidentes de seguridad cibernética serán, al menos, las siguientes:*

1. Definir responsabilidades dentro de las áreas de gestión para facilitar su resolución y la coordinación entre todas las partes que la integran.
2. Establecer las directrices operativas e informativas durante la situación del incidente.
3. Evaluar las estrategias que se llevan a cabo, las acciones y los resultados.
4. Detectar y prever acontecimientos y pasos a seguir en función del desarrollo de los hechos.
5. Identificar oportunidades de mejora para la gestión de incidentes e implementar estrategias de mejora continua.

***Artículo 38. Clasificación, registro y priorización de los incidentes de seguridad cibernética***

*Las entidades y empresas supervisadas deben clasificar, registrar y priorizar los incidentes de seguridad cibernética, de conformidad con el esquema de clasificación y las categorías de impacto que están establecidos en los lineamientos generales del presente reglamento.*

***Artículo 39. Informes de comunicados de incidentes de seguridad cibernética a las Superintendencias***

*Las entidades y empresas supervisadas deben remitir a las respectivas Superintendencias, informes de comunicados de los incidentes de seguridad cibernética cuando:*

1. presenten un impacto funcional “alto”;
2. presenten un impacto a la información en “violación de la privacidad, violación de la propiedad exclusiva o pérdida de integridad”, o
3. el impacto a la capacidad de recuperación sea “extendido” o “no recuperable”.

*Los informes de comunicados de incidentes de seguridad cibernética deben ser remitidos durante la fase de “Detección y análisis” y la fase de “Contención, mitigación y recuperación”, según corresponda.*

*Los tipos de informes de comunicados de incidentes de seguridad cibernética, los plazos y los formatos para su remisión están establecidos en los lineamientos generales del presente reglamento.*

*Las Superintendencias comunicarán, mediante acto administrativo, los canales de remisión de los informes de comunicados de los incidentes de seguridad cibernética.*

***Artículo 40. Comunicado de incidentes a los clientes***

*Cuando la confidencialidad o integridad de la información de los clientes sea afectada debido a un incidente de seguridad cibernética, las entidades y empresas supervisadas deberán comunicarles a estos sobre la afectación. Será responsabilidad de las entidades y empresas supervisadas definir el tipo, el alcance y el contenido mínimo de la comunicación, la cual, deberá ser oportuna, clara y con un alcance apropiado en función del incidente.*

*Las medidas adoptadas para remediar el incidente se deben comunicar a los clientes en un plazo máximo de dos días hábiles posteriores al cierre del incidente.*

***Artículo 41. Reporte histórico de incidentes***

*Las entidades y empresas supervisadas deben remitir a las respectivas Superintendencias un reporte histórico de los incidentes de seguridad cibernética cerrados que tuvieron un impacto funcional de sus sistemas de TI “medio” y “alto”, los cuales presenten un impacto de “pérdida de integridad” de la información o que el impacto a la capacidad de recuperación sea “complementado”, “extendido” o “no*

*recuperable”.*

*El contenido, los canales y los plazos de remisión del reporte están establecidos en los lineamientos generales del presente reglamento.*

## CAPÍTULO V

## LA AUDITORÍA EXTERNA DE TI

### *Sección I. Perfil tecnológico*

***Artículo 42. Perfil tecnológico***

*Las entidades y empresas supervisadas deben elaborar su perfil tecnológico y actualizarlo anualmente.*

*En los casos en que se cuente con una gestión de TI corporativa, un Comité de TI corporativo o sus respectivas funciones equivalentes a nivel corporativo, el grupo o conglomerado financiero podrá remitir un único perfil tecnológico al supervisor responsable.*

*En cualquier caso, el perfil debe ajustarse al marco de gobierno y de gestión de TI de las entidades y empresas supervisadas que conforman el grupo o conglomerado e identificará las particularidades de cada una de estas.*

*El contenido del perfil tecnológico y la guía para la descarga, llenado y remisión vigentes se encuentran en los sitios electrónicos oficiales de cada Superintendencia. Los plazos y los canales de remisión del perfil tecnológico están establecidos en los lineamientos generales del presente reglamento.*

***Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI***

*Las entidades y empresas supervisadas deben indicar en el perfil tecnológico cuáles de los procesos de evaluación detallados en los lineamientos generales del presente reglamento resultan adecuados a su marco de gobierno y gestión de TI. Asimismo, las entidades y empresas supervisadas deberán indicar, en el perfil tecnológico, los procesos de evaluación que no les apliquen, así como los que estén externalizados de forma total o parcial.*

*Los procesos de evaluación que no les apliquen deben estar debidamente fundamentados en un estudio técnico, el cual debe ser remitido mediante los canales oficiales de comunicación de cada Superintendencia. Los* *aspectos que deben ser considerados para la elaboración del estudio técnico están establecidos en los lineamientos generales del presente reglamento.*

*Sin perjuicio de lo anterior, mediante acto administrativo, las Superintendencias podrán ampliar la cantidad de procesos de evaluación declarados en el perfil tecnológico de acuerdo con las necesidades de supervisión, el riesgo identificado o cuando se determine que el marco de gobierno y gestión de TI no es acorde con las particularidades de las entidades o empresas supervisadas.*

*Los criterios de calificación de los procesos de evaluación del marco de gobierno y gestión de TI están establecidos en el anexo 3 de los lineamientos generales del presente reglamento.*

***Artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética***

*Las entidades y empresas supervisadas deben indicar en el perfil tecnológico cuáles categorías de las funciones de la seguridad cibernética establecidas en el anexo 4 de los lineamientos generales del presente reglamento resultan adecuadas para evaluar su gestión de riesgos de seguridad cibernética.*

*Las entidades y empresas supervisadas diseñarán e implementarán los controles relacionados con las funciones de seguridad cibernética y sus categorías, de conformidad con los estándares internacionales, marcos de referencia y mejores prácticas relacionadas con la seguridad cibernética que consideren adecuados para mitigar sus riesgos y alineándolas al sistema de gestión de la seguridad de la información a través de la declaración de aplicabilidad.*

***Artículo 45. Comunicación de cambios significativos del perfil tecnológico***

*Cuando se presenten cambios significativos en el perfil tecnológico con respecto al perfil anterior remitido a la Superintendencia, las entidades y empresas supervisadas deben comunicar dichos cambios.*

*El plazo y los canales de comunicación de los cambios significativos del perfil tecnológico están establecidos en los lineamientos generales del presente reglamento.*

### *Sección II. Auditoría externa de TI*

***Artículo 46. Auditoría externa de TI***

*Las Superintendencias solicitarán a las entidades y empresas supervisadas la contratación de una auditoría externa de TI sobre el marco de gobierno y gestión de TI según el alcance determinado por el supervisor.*

*Además, las Superintendencias, según los riesgos identificados, podrán solicitar a las entidades y empresas supervisadas la contratación de auditorías externas de TI para sus proveedores de bienes y servicios de TI.*

*La auditoría externa de TI deberá ser realizada de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA.*

*Las entidades y empresas supervisadas deben cumplir con lo dispuesto en el Reglamento General de Auditores Externos, Acuerdo CONASSIF 1-10, para la contratación de las auditorías externas de TI.*

***Artículo 47. Alcance y plazo de la auditoría externa de TI***

*Las Superintendencias deben comunicar a las entidades y empresas supervisadas, el alcance de la auditoría externa de TI, el cual podrá considerar, al menos, los siguientes aspectos:*

1. Los procesos de evaluación del marco de gobierno y gestión de TI establecidos en los lineamientos generales del presente reglamento, aplicables en el momento de la solicitud de la auditoría externa de TI.
2. Las funciones para la evaluación de la gestión de riesgos de seguridad cibernética establecidas en los lineamientos generales del presente reglamento.
3. Componentes revelados en el perfil tecnológico de la entidad o empresa supervisada.
4. Entidades y empresas supervisadas, así como áreas de negocio y áreas de TI por considerar en cada proceso.
5. Proveedores de bienes y servicios de TI que, según los riesgos identificados, requieran la evaluación de una auditoría externa de TI.
6. El periodo de cobertura.
7. Aspectos que las Superintendencias requieran de conformidad con los riesgos identificados.

*Cuando la gestión de TI, el Comité de TI o sus respectivas funciones equivalentes sean corporativos, le corresponde a los Órganos de Dirección asegurar que la atención del alcance de la auditoría externa incluya lo que corresponde a cada una de las entidades y empresas supervisadas, de tal forma, que los productos por entregar evalúen el gobierno y la gestión de TI a nivel de los procesos y los riesgos del negocio que desarrolla cada entidad o empresa supervisada.*

*El plazo para la auditoría externa de TI y los canales de remisión del alcance están establecidos en los lineamientos generales del presente reglamento.*

***Artículo 48. Periodicidad de las auditorías externas de TI***

*La periodicidad de la auditoría externa será cada dos años, excepto, cuando el supervisor considere con base en el perfil de riesgo o los resultados de la supervisión, la necesidad de anticiparla o aplazarla.*

***Artículo 49. Documentación sobre la contratación y la planificación de la auditoría externa de TI***

*Las entidades y empresas supervisadas deben remitir a las Superintendencias, la documentación sobre la contratación y la planificación de la auditoría externa de TI, la cual, debe incluir al menos:*

1. la copia del contrato suscrito por los servicios de auditoría, y
2. la planificación del encargo.

*El formato de la planificación del encargo, así como el plazo y los canales para la remisión de la documentación sobre la contratación y la planificación de la auditoría externa de TI, están establecidos en los lineamientos generales del presente reglamento.*

***Artículo 50. Productos de la auditoría externa de TI***

*Las entidades y empresas deben remitir a la respectiva Superintendencia los siguientes productos de la auditoría externa de TI:*

1. El informe de la auditoría externa de TI.
2. La copia del acuerdo del Órgano de Dirección en el que se aprobó el informe de la auditoría externa de TI. Se debe indicar el número y fecha del acta en la que se consignó el acuerdo.
3. La matriz de evaluación del marco de gobierno y gestión de TI.
4. Cualquier otro producto solicitado por la Superintendencia en el alcance de la auditoría externa de TI.

*Los formatos, características y canales de remisión de los productos de la auditoría externa de TI están establecidos en los lineamientos generales del presente reglamento.*

***Artículo 51. Presentación de los resultados de la auditoría externa de TI***

*Las entidades y empresas supervisadas deben convocar, previa coordinación con la respectiva Superintendencia, una reunión para la presentación de los resultados de la auditoría externa de TI por parte del auditor CISA responsable.*

*Los canales para la coordinación de la reunión, el contenido mínimo de la presentación de los resultados de la auditoría externa de TI y las personas que deben participar están establecidos en los lineamientos generales del presente reglamento.*

### *Sección III. Reporte de supervisión y plan de acción*

***Artículo 52. Reporte de supervisión***

*Las Superintendencias elaborarán un reporte de supervisión para comunicar a las entidades y empresas supervisadas, el resultado de la valoración de los productos de la auditoría externa de TI remitidos, así como los hallazgos y los riesgos identificados.*

*Además, las Superintendencias disponen de un plazo de cuarenta días hábiles contados a partir de la presentación de los resultados de la auditoría externa de TI, para remitir a las entidades o empresas supervisadas el reporte de supervisión.*

*El reporte de supervisión será remitido por medio de los canales oficiales de comunicación de cada Superintendencia.*

***Artículo 53. Inadmisibilidad de los productos de la auditoría externa de TI***

*El supervisor puede declarar inadmisibles los productos de la auditoría externa de TI cuando incumplan las disposiciones establecidas en este reglamento, en sus lineamientos generales o en ambos.*

*En caso de inadmisibilidad, las entidades o empresas supervisadas deben remitir los productos corregidos en el plazo de treinta días hábiles, contados a partir de la fecha de comunicación del reporte de supervisión. Cuando las Superintendencias lo requieran, podrán establecer un plazo menor para la remisión de los productos, el cual, no podrá ser menor a diez días hábiles.*

*El plazo dispuesto para que las Superintendencias remitan nuevamente el reporte de supervisión iniciará a partir de la última recepción de los productos corregidos.*

*Las Superintendencias pueden solicitar una nueva reunión para la presentación de los resultados finales de la auditoría externa de TI.*

***Artículo 54. Plan de acción para la gestión de los hallazgos y los riesgos identificados como resultado de la auditoría externa de TI***

*Las entidades y empresas supervisadas deben elaborar un plan de acción para gestionar los hallazgos y los riesgos que se identifiquen como resultado de la auditoría externa de TI.*

*La aprobación de los planes de acción por parte del supervisor aplicará en aquellos casos en los que así lo defina la regulación específica de cada Superintendencia.*

*Los aspectos sobre la elaboración del plan de acción están establecidos en los lineamientos generales del presente reglamento.*

*El plan de acción debe ser remitido a las Superintendencias en el plazo de treinta días hábiles contados a partir de la comunicación del reporte de supervisión. Cuando las Superintendencias lo requieran, podrán establecer un plazo menor para la remisión del plan de acción, el cual, no podrá ser menor a diez días hábiles.*

*Los supervisores pueden realizar observaciones al plan de acción, sugerir mejoras o advertir sobre los riesgos significativos. Cuando las actividades incluidas en el plan de acción no atienden adecuadamente los hallazgos y los riesgos, la frecuencia de presentación de los informes de avances no permite un adecuado seguimiento al plan de acción, los supervisores solicitarán las modificaciones pertinentes a la entidades o empresas supervisadas.*

### *Sección IV. Prórrogas*

***Artículo 55. Solicitudes de prórrogas***

*Las entidades y empresas supervisadas pueden presentar una solicitud de prórroga ante la respectiva Superintendencia para el plazo de la remisión de los productos de la auditoría externa de TI y para el plazo de la remisión del plan de acción.*

*Las solicitudes de prórroga deben ser presentadas de forma previa al vencimiento del plazo original.*

*Las* *pautas para la elaboración de las solicitudes de prórroga y los canales de remisión están establecidas en los lineamientos generales del presente reglamento.*

***Artículo 56. Aceptación o rechazo de las solicitudes de prórrogas***

*La respectiva Superintendencia valorará los fundamentos presentados en la solicitud de prórroga y aceptará o rechazará dicha solicitud.*

*En caso de aceptación de la solicitud, se comunicará a la entidad o empresa supervisada el plazo adicional concedido mediante los canales oficiales de comunicación de cada Superintendencia.*

## DISPOSICIONES ADICIONALES

### *Disposición adicional primera. Referencias normativas*

*Toda referencia en la reglamentación emitida por el CONASSIF u otras disposiciones de inferior rango emitidas por los superintendentes que hagan referencia al Reglamento General de Gestión de Tecnología de Información, Acuerdo CONASSIF 5-17, debe leerse como Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24.*

## DISPOSICIONES TRANSITORIAS

### *Disposición transitoria primera. Auditorías externas de TI*

*Las Superintendencias podrán realizar visitas de supervisión, solicitudes de trabajos especiales a los Órganos de Control o solicitudes de auditorías externas de TI considerando dentro de los alcances y plazos de dichos trabajos el cumplimiento de las disposiciones establecidas en el presente reglamento a partir de la publicación de sus modificaciones en el diario oficial La Gaceta.*

*La secuencia y los plazos de las auditorías externas iniciadas con base en el Acuerdo CONASSIF 5-17 no serán interrumpidos por la transición a las modificaciones del presente reglamento.*

### *Disposición transitoria segunda. Gestión de TI corporativa*

*Los grupos y conglomerados financieros que, previo a la publicación de las modificaciones del presente reglamento en el diario oficial La Gaceta, hayan tipificado su gestión de TI como corporativa, podrán mantener dicha condición.*

### *Disposición transitoria tercera. Planes de acción vigentes*

*Los planes de acción en curso originados por trabajos de supervisión o como parte de los resultados de las auditorías externas de TI solicitadas en periodos previos a la publicación de las modificaciones del presente reglamento en el diario oficial La Gaceta, deben ser finalizados en tiempo y forma.*

### *Disposición transitoria cuarta. Contratos con proveedores de bienes y servicios de TI*

*Con respecto a los contratos vigentes y futuros suscritos con los proveedores de bienes y servicios de TI, las entidades y empresas supervisadas deben considerar lo siguiente:*

1. Contratos nuevos: A partir de la publicación de las modificaciones del presente reglamento en el diario oficial La Gaceta, deben acatarse las disposiciones sobre contratos y acuerdos de nivel de servicio.
2. Contratos vigentes: Continúan según lo acordado entre las partes. Las disposiciones aplicarán en caso de renovación del servicio y cuando deban suscribir nuevos contratos y acuerdos de nivel de servicio. En todo caso, dicho plazo no podrá exceder los doce meses a partir de la entrada en vigor del presente reglamento.

### *Disposición transitoria quinta. Sociedades corredoras de seguros*

*De conformidad con el requerimiento dispuesto en el artículo 3. Regulación proporcional, las sociedades corredoras de seguros se regirán por las siguientes disposiciones transitorias:*

*1.Marco de gestión de TI de las sociedades corredoras de seguros y periodo de transición:*

*Las sociedades corredoras de seguros deben implementar los procesos de su marco de gestión de TI gradualmente como máximo durante los primeros tres años contados a partir de la entrada en vigor 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, la SUGESE requiere que las sociedades corredoras de seguros implementen su marco de gestión, así como 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 su estrategia de gestión de los riesgos de TI.*

*2.Perfil tecnológico de las sociedades corredoras de seguros:*

1. *Las sociedades corredoras de seguros remitirán su primer perfil tecnológico de TI, a partir del 2025, independientemente del tipo de gestión, comité o unidad de TI sea esta individual o corporativa que la entidad defina.*
2. *Las fechas de remisión del primer perfil de las sociedades corredoras de seguros serán comunicadas por la SUGESE mediante acto administrativo en el tercer trimestre del 2024, a través de los canales oficiales.*

*3.Auditoría Externa de TI:*

*La SUGESE podrá requerir a las sociedades corredoras de seguros, la primera auditoría externa de TI a partir del enero del 2027.*

*Rige a partir de su publicación en el diario oficial La Gaceta.’”*

Atentamente,

Celia Alpízar Paniagua

***Secretaria interina del Consejo***

***Comunicado a:*** *Sistema financiero nacional, Asociación Costarricense de Auditores en Informática (c.a: Superintendencia General de Entidades Financieras, Intendencia Sugef y Auditoría Interna).*