17 de abril del 2024
CNS-1853/06
CNS-1854/05

Señora
Laura Suárez Zamora, presidente
Consejo Nacional de Supervisión del Sistema Financiero

Estimada señora:

El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 6 y 5 de las actas de las sesiones 1853-2024 y 1854-2024, celebradas el 16 de abril del 2024,

considerando que:

A. 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.

B. 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 diez 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

I. 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".

II. 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.

III. 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.

IV. 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.

V. 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.

VI. 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.

VII. 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.

VIII. 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.

IX. 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.

X. 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.

XI. 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

XII. 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:

a. 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.

b. *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 de la información, 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

XIII. 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.

XIV. 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

XV. 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 de la información y* seguridad cibernética.

consideraciones sobre la gestión de la tecnología de información

XVI. 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.

XVII. 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

XVIII. 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 de la información y* seguridad cibernética, ya que se deben considerar las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la

nube. Lo anterior, en función del tipo de modelo de implementación y el tipo de servicio de computación en la nube adquirido.

XIX. Es importante que las entidades y empresas supervisadas tengan definido las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube, aplicables para cada uno de los modelos de implementación y los tipos 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

XX. 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 la seguridad de la información, así como de la 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 de la información y* seguridad cibernética de los proveedores son elementos críticos.

XXI. Los proveedores de bienes y servicios de TI y su cadena de suministro no están dentro del alcance de esta regulación; sin embargo, es necesario que las entidades y empresas supervisadas asuman su responsabilidad en 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, través de mecanismos de control, tales como: 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, aceptación de términos y condiciones de la organización por parte de terceros, auditorías externas, informes de aseguramiento, entre otros.

XXII. 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 de la información y* 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

XXIII. 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.

XXIV. 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.

XXV. 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.

XXVI. 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.

XXVII. Es importante que las entidades y empresas supervisadas cuenten con un marco regulatorio que contemple las buenas prácticas en materia de *seguridad de la información y* 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.

XXVIII. 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

XXIX. 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.

XXX. 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) emitida por ISACA, 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

XXXI. 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.

XXXII. Las asociaciones profesionales, entidades globales, gobiernos de diferentes jurisdicciones, así como diferentes industrias 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.

XXXIII. El marco de referencia COBIT 2019, emitido por ISACA, 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.

XXXIV. 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, los Controles CIS del *Center for Internet Security* y los controles del *Cloud Security Alliance*.

XXXV. 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

XXXVI. 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

XXXVII. 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.

XXXVIII. El Acuerdo Conassif 5-17 es una normativa transversal, que resulta de aplicación para los regulados de la Sugef, la Sugeval, la Supen y la Sugese.

Considerando que el Conassif que conoce temas de Supen se encuentra parcialmente desintegrado, por estar pendiente el nombramiento del representante de la Asamblea de Trabajadores del Banco Popular y de Desarrollo Comunal, debido a que el nombramiento del señor Álvaro Enrique Ramírez Sancho fue dispuesto por la Junta Directiva del Banco Central de Costa Rica en el artículo 5 de la sesión número 5857-2018 de 12 de diciembre de 2018, por cinco años, concluyendo, como es sabido, el día 14 de diciembre de 2023, es necesario que para los

regulados del sector pensiones esta reforma sea adoptada utilizando para ello la teoría del funcionario de hecho.

Al respecto, y atendiendo a una consulta formulada por Conassif, debido también a la falta de nombramiento del representante de la Asamblea de Trabajadores del Banco Popular y de Desarrollo Comunal, en el criterio C-100-2011 del 3 de mayo de 2011, la Procuraduría General de la República explica que:

> *"En el caso que nos ocupa, el Consejo está bien integrado para su funcionamiento general y en relación con otras Superintendencias. Empero, no lo está cuando se trata de conocer asuntos específicos relacionados con la competencia de la Superintendencia de Pensiones.* ***Competencias todas que son indispensables*** *para el correcto funcionamiento no solo de la Superintendencia de Pensiones sino del sistema de pensiones del país en general.* ***Es el caso del ejercicio de la potestad reglamentaria*** *y de la sancionadora y, en general, aquellas en que se manifiesta la regulación del sector pensiones. Importa recalcar que si el Consejo Nacional de Supervisión del Sistema Financiero no se constituye en los términos del artículo 35 de la Ley 7523, no puede conocer de estas facultades en relación con la Superintendencia de Pensiones, con lo que esta no podría actuar sus competencias, satisfaciendo el interés público que justifica su existencia.* ***Con lo cual se arriesgaría, obviamente, el orden público económico que impregna toda la regulación y supervisión del sistema financiero en general y del de pensiones, en particular****." [Lo resaltado no es del original].*

No obstante, en dicho criterio se reconoce que:

> *"Resulta incuestionable que el resguardo de los derechos e intereses de los trabajadores beneficiarios del sistema de pensiones, así como la estabilidad y solvencia del sistema financiero en su conjunto* ***requieren la continuidad del funcionamiento del CONASSIF y de la SUPEN****. Continuidad que, repetimos, se ve afectada cuando el órgano colegiado, CONASSIF, no está debidamente integrado para conocer de los asuntos regulatorios en materia de pensiones y, por ende, para actuar las competencias respectivas.* ***Consecuencia que puede evitarse con la aplicación de la teoría del funcionario de hecho*** *[...]". [Lo resaltado no es del original].*

Ahora bien, la Procuraduría concluye que:

> *"El Consejo Nacional de Supervisión del Sistema Financiero puede recurrir a la figura del funcionario de hecho a efecto de emitir el acto previsto por la Ley,* ***en situaciones de evidente riesgo de ese orden público económico y social****".* Y agrega: *"Es entendido que la actuación del funcionario de hecho debe tender a la satisfacción general y a la concreción de los fines a que se refiere el orden público a que se ha hecho referencia, en particular la protección de los derechos e intereses de los trabajadores garantizados por la Ley de Protección al Trabajador".* [Lo resaltado no es del original].

Se justifica que la propuesta de modificación integral del Acuerdo Conassif 5-17 sea adoptada para los regulados por la Superintendencia de Pensiones, recurriendo para ello a la teoría de funcionario de hecho, por las siguientes razones:

a) Los ataques cibernéticos representan una amenaza creciente en frecuencia y sofisticación, con impactos disruptivos para la continuidad del negocio y la integralidad de la información, con efectos perjudiciales para la estabilidad de las entidades financieras y del Sistema Financiero Nacional. Esta realidad, evidencia la necesidad imperiosa de que, a nivel reglamentario, se requiera a las entidades financieras un marco robusto de gestión del riesgo de seguridad cibernética, teniendo en cuenta, además, el alto grado de interconexión entre ellas y la existencia de entidades de importancia sistémica.

b) Las vulnerabilidades de seguridad de la información y seguridad cibernética de los proveedores de bienes y servicios de TI podrían convertirse en canales de ataque a las entidades supervisadas, por lo que, las capacidades de seguridad de dichos proveedores son elementos críticos, y se requiere de las entidades supervisadas una gestión diligente de su relación con dichos proveedores.

c) La computación en la nube tiene beneficios, pero también presenta riesgos potenciales, como los relacionados con la seguridad y la confidencialidad de los datos, así como la vulnerabilidad de los sistemas de tecnología de la información (TI) a los ataques cibernéticos.

d) Los incidentes e interrupciones de servicios de TI podrían afectar la operación continua de los procesos críticos para el negocio y la disponibilidad de la información de las entidades supervisadas, así como asegurar la continuidad del proceso de supervisión.

e) La implementación de tecnologías emergentes puede provocar un impacto estratégico en las entidades supervisadas si no se gestionan adecuadamente sus riesgos. Es necesario que la supervisión de TI permita valorar si las entidades están preparadas para aprovechar las ventajas de las innovaciones tecnológicas y gestionar los riesgos asociados.

Lo planteado anteriormente, evidencia la existencia de riesgos que requieren ser abordados a nivel regulatorio, a efecto de que exista un estándar mínimo que deban observar las entidades financieras en sus operaciones. Claramente, la inadecuada gestión de esos aspectos, así como de otros que están contemplados en el reglamento, tienen la virtud de poder afectar seriamente al sistema financiero, a las entidades mismas, así como al orden público económico y social.

Finalmente, y por tratarse de una norma transversal, resulta indispensable que la modificación propuesta se apruebe no solo para los regulados por la Sugef, la Sugeval y la Sugese; este cambio debe ser aprobado también para los regulados por la Supen con el propósito de asegurar un trato uniforme con el resto de las empresas y entidades supervisadas de los grupos y conglomerados financieros y para evitar los espacios de asimetría regulatoria, que se podrían generar como consecuencia de la aplicación de una regulación desigual entre las entidades supervisadas del sistema financiero, sin que exista una justificación técnica para ello.

Conviene agregar que, desde larga data, la Sala Constitucional se ha pronunciado sobre la validez de las actuaciones emanadas de los funcionarios de hecho, de cumplirse los presupuestos establecidos en las normas atinentes de la Ley General de la Administración Pública. Así, en el voto 1593-94 indicó que:

> *"Esta Sala ha aceptado válidamente, la aplicación de la teoría del funcionario de hecho, estipulada en la Ley General de la Administración Pública, en sus artículos 155 y siguientes. En reiteradas ocasiones, (vid sentencias N.° 2765-92, 15:30 horas del 01-09-92 y N.° 6701-93, 15:06 del 21-12-93) ha manifestado que*

> *las actuaciones realizadas por un funcionario de hecho, revisten su carácter de validez en tanto se cumplan determinados requisitos o condiciones,* ***ello con la necesidad de preservar el interés general, mismo que constituye el principal objetivo que ha de ser atendido por el ordenamiento jurídico****. Por lo que acerca de los requisitos para reconocer la validez de los actos de los funcionarios de hecho, se encuentra este tribunal los siguientes:*
>
> *´ ... Que exteriormente se presenten como si emanaran de funcionarios de jure, es decir, deben producir, respectos a terceros, al público, los efectos jurídicos propios de los actos que emanan de agentes verdaderamente regulares...* ***El reconocimiento de la validez de esos actos en favor de los terceros, debe ser "de interés público", en busca de la seguridad jurídica y la certidumbre del derecho...*** *También es necesario que lo actuado por el funcionario de hecho se haya realizado dentro de los límites de competencia de la autoridad oficial que dicho funcionario pretende tener...´ (Sentencia número 6701-93)". [Lo resaltado no es del original].*

Por su parte, en el criterio C-100-2011, arriba mencionado, la Procuraduría General de la República reafirma el carácter de interés público de que revista la regulación financiera, como sigue:

> ***"El carácter de interés público de la regulación financiera es indiscutible y se origina en el hecho mismo, repetimos, que las entidades financieras actúan en el mercado, captando, manejando, invirtiendo el*** *ahorro* ***de terceros. De allí la necesidad de regular que las entidades no incurran en riesgos que lesionan el interés de los ahorrantes o inversionistas.***
>
> *Por ese poder de policía de contenido financiero, se permite a los órganos regulador y supervisor reglamentar la actividad financiera y los agentes que en ella intervienen, dictando normas que permiten interpretar e integrar las leyes en la materia, vigilar el funcionamiento del sistema y aplicar esas leyes; en su caso, sancionar el irrespeto al régimen especial. De esa forma, se orienta y dirige la actividad financiera necesaria para atender las necesidades de la producción y el consumo, así como satisfacer los intereses de los inversionistas o ahorrantes. Importa destacar que se reconoce la posibilidad de imponer reglas de comportamiento a los intermediarios financieros, tendientes a prevenir que incurran en riesgos excesivos y a garantizar la solvencia y la liquidez de los establecimientos. El objetivo último: la estabilidad y solvencia de los distintos agentes financieros y del sistema en general". Dictamen N. C-320-2005 de 6 de setiembre de 2005.*
>
> *A la estabilidad y solvencia de los entes supervisados por la Superintendencia de Pensiones,* ***se une la finalidad social propia del régimen de pensiones,*** *que no es otra que la protección del trabajador y ex trabajador en caso de invalidez, vejez y muerte. […]" [Lo resaltado no es del original].*

XXXIX. Mediante artículos 4 y 5 de las actas de las sesiones 1834-2023 y 1835-2023, celebradas el 20 de noviembre del 2023, el Conassif remitió a consulta pública 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, las entidades del Sistema Financiero Nacional podían enviar al Despacho de la superintendente general de entidades financieras sus

comentarios y observaciones. Posteriormente, mediante artículos 6 y 4 de las actas de las sesiones 1837-2023 y 1838-2023, celebradas el 4 y 6 de diciembre del 2023, el Conassif dispuso extender, al 15 de enero del 2024, el plazo para la recepción de comentarios y observaciones a la citada propuesta de modificación normativa remitida en consulta.

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:

a) Supervisados por SUGEF:

1. *Bancos comerciales del Estado*
2. *Bancos creados por ley especial*
3. *Bancos privados*
4. *Empresas financieras no bancarias*
5. *Organizaciones cooperativas de ahorro y crédito*
6. *Mutuales de ahorro y préstamo*
7. *Caja de Ahorro y Préstamos de la ANDE*

b) Supervisados por SUGEVAL:

1. *Puestos de bolsa y sociedades administradoras de fondos de inversión*
2. *Bolsas de valores*
3. *Sociedades de compensación y liquidación*
4. *Proveedores de precio*
5. *Entidades que brindan servicios de custodia*
6. *Centrales de valores*
7. *Sociedades titularizadoras y fiduciarias*
8. *Entidades de registros centralizados de letras de cambio y pagarés electrónicos*

c) Supervisados por SUGESE:

1. *Entidades aseguradoras y reaseguradoras*

2. *Sucursales de entidades aseguradoras extranjeras*
3. *Sociedades corredoras de seguros*

d) Supervisados por SUPEN:

1. *Operadoras de pensiones complementarias*
2. *Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social*
3. *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.

e) 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 en función de sus riesgos, tamaño, complejidad y modelo de negocio: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información.*

2. *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: a) El artículo 33. Programas de análisis de vulnerabilidades y pruebas, b) El artículo 34. Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de seguridad cibernética y en c) El artículo 35. Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética, del presente reglamento.*
   Los artículos 33, 34 y 35 se consideran como referencias sobre sanas prácticas que las entidades, discrecionalmente, podrán adoptar en función de sus riesgos, tamaño, complejidad y modelo de negocio.

3. *Lo dispuesto en el Capítulo V La auditoría externa de TI, será de aplicación plena, salvo lo dispuesto en: a) El artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI, b) El artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética y, c) El artículo 47. Alcance y plazo de la Auditoría Externa de TI, inciso b).*

   Además, las entidades, en función de su perfil de riesgo y de la naturaleza de sus operaciones, deberán gestionar TI y sus riesgos relacionados. A fin de evaluar dicha gestión, las entidades deben considerar los siguientes aspectos:

a) Las entidades definirán el alcance de la auditoría externa estableciendo los procesos de evaluación que consideren pertinentes en función de sus riesgos y modelo de negocio, según el anexo 1 de los lineamientos generales del presente reglamento.

b) 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.

Artículo 4. Definiciones y abreviaturas

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

*a) **Activos digitales**: Todo tipo de datos o activos de información que se presenten en formato digital, los cuales, sean propiedad de una entidad o empresa supervisada o de sus partes interesadas y que permiten a estas mantener sus operaciones digitales y tecnológicas.*
*b) **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, reputación o el ecosistema financiero.*
*c) **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.*
*d) **Gestión de TI**: Conjunto de estructura de relaciones y procesos para planificar, construir, ejecutar y monitorear la tecnología de la información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.*
*e) **Gobierno de TI**: Subcomponente del gobierno corporativo, el cual, se encarga de la evaluación, dirección y supervisión de las tecnologías de información.*
*f) **ISACA**: Acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association).*
*g) **Marco de gobierno y gestión de TI**: Conjunto de procesos destinados a gobernar y gestionar las tecnologías de información de las entidades y empresas supervisadas, los cuales, deben ser adoptados y adaptados para gobernar y gestionar de forma integral los riesgos relacionados con las tecnologías e información, 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.*
*h) **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.*
*i) **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.*
*j) **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.*
*k) **Proveedores de bienes y servicios de TI críticos**: Persona física o jurídica que provee bienes o servicios de TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).*
*l) **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.

m) ***Seguridad cibernética**: Práctica de gestionar los riesgos para 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.*

n) ***Seguridad de la información**: Práctica de gestionar los riesgos que afectan los objetivos de confidencialidad, integridad y disponibilidad de la información requeridos por la organización para el uso de las personas, procesos y tecnologías de la información en los procesos y servicios de negocio.*

o) ***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.*

p) ***Unidad de TI o función equivalente**: Instancia o 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, la tolerancia y la capacidad de riesgo; el tamaño, complejidad, modelo de negocio 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.

El marco de gobierno y gestión de TI puede ser implementado en las unidades de TI, en las áreas de negocio o ser externalizado mediante servicios.

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:

a) Orientar hacia la definición del gobierno de TI con un enfoque integrado y alineado con el gobierno corporativo.
b) Asegurar un equilibrio entre el uso de los recursos de TI y los procesos críticos de negocio.
c) Crear valor mediante los beneficios de las tecnologías de información, dentro de los márgenes de apetito, tolerancia y capacidad de riesgo.
d) Asegurar que la entidad o empresa supervisada dispone de recursos adecuados y suficientes para el gobierno y la gestión de TI.
e) Asegurar que se identifica e involucra a las partes interesadas en el diseño del marco de gobierno y gestión de TI.
f) Diseñar e implementar el marco de gobierno y gestión de TI de conformidad con los objetivos y riesgos del negocio.
g) Asegurar que la planificación estratégica de TI permita una visión holística de la entidad o empresa supervisada en su entorno actual, así como de su dirección futura.
h) Establecer una dirección y una estructura eficiente para gestionar TI; además, alinear los objetivos de la entidad o empresa supervisada con el uso de la tecnología y su arquitectura organizacional.
i) Gestionar la innovación, las tecnologías emergentes, el conocimiento y los datos relacionados con la entidad o empresa supervisada.
j) Gestionar el presupuesto, los costos, el conocimiento y el recurso humano de la unidad de TI, así como las relaciones con las partes interesadas.
k) Establecer la gestión de los acuerdos de nivel de servicio, de los proveedores de bienes y servicios de TI, así como la gestión de los riesgos de TI de manera holística en la entidad o empresa supervisada.
l) Establecer el 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.
m) Definir la gestión del portafolio, de los programas y de los proyectos de TI que permitan atender la definición de los requisitos del negocio.
n) Determinar la estrategia de adquisición, construcción e implementación de soluciones tecnológicas integradas al negocio.
o) Gestionar la disponibilidad y la capacidad de infraestructura tecnológica, así como asegurar la continuidad de las operaciones.
p) Asegurar la configuración de los activos de información de conformidad con la gestión, aceptación y transición de los cambios.
q) Gestionar las operaciones de TI, los incidentes, la solución de los problemas de TI, los servicios de seguridad de la información y de seguridad cibernética, así como los controles de los procesos del negocio; además, asegurar una resiliencia operativa digital.
r) Gestionar el monitoreo del desempeño y la conformidad de los procesos, del sistema de control interno, del cumplimiento de los requisitos externos, así como del cumplimiento normativo, la legislación nacional aplicable y del aseguramiento de TI.

El cumplimiento de dichos propósitos debe ser de conformidad con la estrategia organizacional, los riesgos, el tamaño, la complejidad y el modelo de negocio de las entidades y empresas supervisadas.

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:

a) Aprobar el marco de gobierno y gestión de TI, así como asegurar que la declaración de apetito de riesgo incorpore el apetito, la tolerancia y la capacidad de los riesgos asociados a TI.
b) Establecer un Comité de TI o una función equivalente y aprobar sus normas de gobierno y gestión.

c) Aprobar las políticas, estructuras, estrategias, recursos, inversiones y presupuestos necesarios para la implementación del marco de gobierno y gestión de TI, así como para las tecnologías emergentes que se implementen.
d) Aprobar los informes de la auditoría externa de TI que serán remitidos a las Superintendencias.
e) 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.
f) Asegurar que se consideren 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.
g) Designar las áreas de negocio y de TI responsables de diseñar e implementar el marco de gobierno y de gestión TI.

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:

a) 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.
b) Promover las discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética en las reuniones del Órgano de Dirección.
c) Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles.
d) Aprobar los planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética.

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:

a) Aprobar las políticas de resiliencia operativa digital de la entidad o empresa supervisada.
b) Asegurar que la resiliencia operativa digital esté incorporada dentro de los planes de contingencia y continuidad de negocio.
c) Aprobar los presupuestos y recursos necesarios para asegurar la resiliencia operativa digital.
d) Asegurar que se implementen planes de respuesta, recuperación y atención de crisis para gestionar los incidentes relacionados con los activos digitales que podrían interrumpir la ejecución de los procesos críticos.
e) Asegurar que los planes de respuesta de incidentes relacionados con los activos digitales sean acordes con el apetito, tolerancia y capacidad de riesgo establecidos 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:

a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección.
b) Proponer al Órgano de Dirección la estrategia y los recursos requeridos para la implementación del marco de gobierno y gestión de TI.
c) Implementar las políticas relacionadas con TI aprobadas por el Órgano de Dirección.

d) Implementar los planes de acción para la atención de los hallazgos de la auditoría externa de TI.
e) 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, almacenada o procesada por terceros.
f) Establecer las medidas para la gestión de los incidentes de seguridad de la información y seguridad cibernética.
g) 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 sus proveedores de bienes y servicios de TI.
h) Asegurar que la gestión de los datos de la entidad o empresa supervisada se realice de manera efectiva y eficiente; asimismo, que las necesidades de confidencialidad, integridad, disponibilidad, no repudio y auditabilidad, sean atendidas, en función de sus riesgos.

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:

a) Supervisar la implementación del marco de gobierno y gestión de TI.
b) 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.
c) Proponer al Órgano de Dirección las políticas relacionadas con TI.
d) 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.
e) Validar que los procedimientos, los instructivos y la documentación de TI sean implementados desde las unidades funcionales responsables de ejecutarlos.
f) Recomendar al Órgano de Dirección las prioridades para las inversiones en TI.
g) 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.
h) 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, como parte de la planificación de los estudios de la auditoría interna y su universo auditable, al menos, debe:

a) Revisar y asegurar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.
b) 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.
c) Evaluar la calidad y eficacia de los planes de acción elaborados por la entidad o empresa supervisada que atenderán los hallazgos que se identifiquen como resultado de la auditoría externa de TI.
d) 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:

a) Incorporar la gestión de los riesgos tecnológicos, de tecnologías emergentes, de la seguridad de la información y de la seguridad cibernética dentro de la gestión de riesgos de la entidad o empresa supervisada.
b) Incorporar el apetito, la tolerancia y la capacidad de los riesgos tecnológicos, de tecnologías emergentes, de seguridad de la información y de seguridad cibernética dentro de la declaración de apetito de riesgo de la entidad o empresa supervisada.
c) 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:

a) Ejecutar las estrategias para la implementación del marco de gobierno y gestión de TI.
b) Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos establecidos.
c) Diseñar e implementar la arquitectura tecnológica y de aplicaciones alineada a la arquitectura de negocio y a la arquitectura de información, a fin de soportar las operaciones de la entidad o empresa supervisada.
d) Establecer los controles para el desarrollo del ciclo de vida de los servicios, de las aplicaciones, de los sistemas de información y de las soluciones tecnológicas, los cuales, aseguren la confidencialidad, integridad, disponibilidad, calidad, mantenimiento y los cambios por excepción o de emergencia.
e) Asegurar que los bienes y servicios de TI críticos estén identificados; además, asegurar que se mantengan disponibles y que sean gestionados de manera efectiva y eficiente.
f) Asegurar que los requerimientos de las entidades y empresas supervisadas sean atendidos de manera equitativa y en función de los riesgos de cada entidad o empresa que constituye el grupo o conglomerado cuando la gestión de TI sea tipificada como corporativa.

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

Artículo 19. Clasificación de activos de información y del acceso y uso de los datos

Las entidades y empresas supervisadas deben clasificar sus activos de información de conformidad con el modelo de clasificación establecido en los lineamientos generales del presente reglamento.

Las entidades y empresas supervisadas deben etiquetar los activos de información según su nivel de confidencialidad, de conformidad con el modelo de clasificación de acceso y uso de los activos de información y datos establecido en los lineamientos generales del presente reglamento.

Los activos de información primarios y de soporte deben ser revelados en el perfil tecnológico de conformidad con lo establecido en los lineamientos generales del presente reglamento.

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

Las entidades y empresas supervisadas deben poner a disposición de las Superintendencias para sus labores de supervisión, sin ningún tipo de restricción o condición, 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.

Cuando existan bases de datos compartidas entre las entidades y empresas integrantes del grupo o conglomerado financiero, debe efectuarse una separación del registro de las operaciones de cada entidad y empresa integrante del grupo o conglomerado financiero. Asimismo, las bases de datos solo pueden ser utilizadas o compartidas guardando la confidencialidad de la información y la protección de los datos de acuerdo con las normas y las disposiciones legales aplicables.

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 las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube.

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:

a) Gestionar los riesgos derivados del uso de servicios de computación en la nube.
b) Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube. Dichos criterios deben considerar, al menos, la seguridad, fiabilidad, escalabilidad, costo, soporte, experiencia, interoperabilidad y cumplimiento regulatorio.
c) Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001. Además, de conformidad con el servicio externalizado, verificar que cumpla con estándares o buenas prácticas, tales como las ISO 27017, 27018 o las mejores prácticas del Cloud Security Alliance.
d) Asegurar que los niveles de disponibilidad estén de conformidad con los objetivos de resiliencia (RPO y RTO) establecidos por la entidad o empresa supervisada.
e) Establecer controles para asegurar la disponibilidad acordada del servicio con el proveedor.
f) Establecer mecanismos que permitan contar con respaldo de la información que se procesa y almacena 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. Lo anterior, cuando los servicios contratados, por su naturaleza, no garanticen o incluyan el respaldo.

g) Mantener cifrada la información, cuyo uso o acceso esté clasificado como confidencial y sensible, ya sea en tránsito o en reposo, mediante el empleo de estándares y algoritmos reconocidos como seguros de acuerdo con los estándares y mejores prácticas internacionales.

h) 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.

i) Contar con sistemas de registro, monitoreo y alarma de eventos e incidentes de seguridad de la información y seguridad cibernética.

j) Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente.

k) 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.

l) Contar con canales de comunicación con el proveedor de servicios en la nube, cifrados de extremo a extremo, y que, en lo posible, utilicen mecanismos de redundancia.

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

Cuando las entidades y empresas supervisadas dispongan de sus componentes tecnológicos mediante el uso de servicios de computación en la nube, deberán mantener actualizada y a disposición de las Superintendencias la documentación de los controles administrativos y técnicos dispuestos para dichos servicios.

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.

Las entidades y empresas supervisadas deben establecer controles a fin de comprobar que los proveedores que les suministran bienes y servicios de TI implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital, de conformidad con los requerimientos definidos por las 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 dichos bienes y servicios, a su vez, sean subcontratados por los terceros, se cuente con controles de seguridad de la información y seguridad cibernética, asimismo, que se cuente con planes de continuidad del negocio.

Cuando se delegue a terceros el procesamiento, la transmisión o el almacenamiento de información clasificada como confidencial o sensible, las entidades y empresas supervisadas deben asegurar que dichos terceros implementen controles de seguridad de la información y seguridad cibernética.

Artículo 26. Identificación de la información y de los 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.

Las entidades y empresas supervisadas deben establecer procedimientos que permitan mantener identificada la información clasificada como confidencial o sensible que sea procesada, transmitida o almacenada por terceros.

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

Las entidades y empresas supervisadas deben identificar, evaluar y monitorear, de conformidad con sus políticas establecidas, los riesgos de tercerización de la información clasificada como confidencial o sensible, así como los riesgos de tercerización de bienes y servicios de TI críticos. Además, se deben revelar dichos riesgos en el perfil tecnológico.

Artículo 28. Acuerdos de confidencialidad

Las entidades y empresas supervisadas que deleguen a terceros, bienes y servicios de TI que involucren el procesamiento, la transmisión o el almacenamiento de información, deben establecer mecanismos de control tales como los acuerdos de confidencialidad previo al intercambio de información con dichos terceros.

Cuando se celebren contratos de adhesión con terceros, las entidades y empresas supervisadas deben asegurar la confidencialidad de la información, para lo cual podrán utilizar mecanismos de control distintos a los acuerdos de confidencialidad.

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. Además, los acuerdos de nivel de servicio podrán estar incluidos en los contratos, según la naturaleza del bien o servicio externalizado.

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

Las entidades y empresas supervisadas deberán diseñar sus contratos y acuerdos de nivel de servicio de TI, de conformidad con la naturaleza y el riesgo del bien o servicio tercerizado, así como el tipo de proveedor. Mediante lineamientos generales del presente reglamento se establecen elementos a considerar para el diseño de los contratos y acuerdos de nivel de servicio, salvo en los casos en que se trate de bienes o servicios suministrados por proveedores de computación en la nube o contratos de adhesión.

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 que las Superintendencias tengan acceso a los registros, datos e información de los bienes y servicios de TI tercerizados según sean requeridos como parte de los procesos de supervisión.

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 de la información y 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 de la seguridad cibernética. Los controles deberán ser incluidos en 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.

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 la seguridad de la información y la 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 de la información y 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.

Las unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestiones los riesgos de seguridad cibernética 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 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 de la información y seguridad cibernética

Artículo 36. Gestión de incidentes de seguridad de la información y seguridad cibernética

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

Cuando se identifique una brecha de seguridad de información o de seguridad cibernética, las entidades y empresas supervisadas deberán establecer el impacto potencial de conformidad con el modelo de clasificación establecido en los lineamientos generales del presente reglamento.

La gestión de incidentes debe establecer un plan de respuesta a incidentes de seguridad de la información y seguridad cibernética, así como los controles que permitan recopilar las evidencias para el análisis forense.

Artículo 37. Función de respuesta a incidentes de seguridad de la información y seguridad cibernética

Las entidades y empresas supervisadas deben establecer una función de respuesta a incidentes de seguridad de la información y 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 de la información y 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 de la información y de seguridad cibernética serán, al menos, las siguientes:

a) Definir responsabilidades dentro de las áreas de gestión para facilitar su resolución y la coordinación entre todas las partes que la integran.
b) Establecer las directrices operativas e informativas durante la situación del incidente de seguridad de la información o de seguridad cibernética.
c) Evaluar las estrategias que se llevan a cabo, las acciones y los resultados.
d) Detectar y prever acontecimientos y pasos a seguir en función del desarrollo de los hechos para erradicar y resolver el incidente de seguridad de la información o de seguridad cibernética.
e) Identificar oportunidades de mejora para la gestión de incidentes de seguridad de la información y seguridad cibernética, así como implementar estrategias de mejora continua.

Artículo 38. Clasificación, registro e impacto de los incidentes de seguridad de la información y seguridad cibernética

Las entidades y empresas supervisadas deben clasificar y registrar los incidentes de seguridad de la información y seguridad cibernética, de conformidad con la clasificación de incidentes y de su impacto, establecidos en los lineamientos generales del presente reglamento.

Artículo 39. Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias

Las entidades y empresas supervisadas deben comunicar a las respectivas Superintendencias los incidentes de seguridad de la información y seguridad cibernética cuando su impacto sea clasificado como "moderado" o "alto".

Las Superintendencias podrán solicitar informes sobre la atención de los incidentes de seguridad de la información o de seguridad cibernética.

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

Las Superintendencias informarán los canales de remisión de los comunicados y de los informes de incidentes de seguridad de la información y 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 de la información o 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.

Además, las medidas adoptadas para remediar el incidente se deben comunicar a los clientes en un plazo máximo de cinco días hábiles posteriores al cierre del incidente.

Artículo 41. Reporte histórico de incidentes de seguridad de la información y seguridad cibernética

Las entidades y empresas supervisadas deben elaborar un reporte histórico de los incidentes de seguridad de la información y seguridad cibernética. El reporte deberá estar a disposición de las Superintendencias cuando estas lo requieran como parte de las labores de supervisión; en dicho caso, las Superintendencias comunicarán los canales de remisión del reporte.

El contenido del reporte está establecido en los lineamientos generales del presente reglamento.

Las Superintendencias comunicarán los canales de remisión del reporte histórico de los incidentes de seguridad de la información y seguridad cibernética.

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.

Mediante lineamientos generales del presente reglamento se establecen los plazos y los canales de remisión del perfil tecnológico, así como aspectos en relación con el contenido del perfil tecnológico y la guía para su descarga, llenado y remisión vigentes.

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.

Cuando la gestión de TI sea tipificada como corporativa, se podrá realizar un único estudio técnico, el cual, considere las particularidades de cada una de las entidades o empresas supervisadas que conforman el grupo o conglomerado financiero.

Sin perjuicio de lo anterior, 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

Las entidades y empresas supervisadas deben identificar los cambios que se realicen en el perfil tecnológico con respecto al perfil anterior, los cuales, consideren que son significativos. Lo anterior, en virtud de su naturaleza, tamaño, complejidad, modelo de negocio y riesgos.

Además, las entidades y empresas supervisadas deben comunicar dichos cambios significativos a las Superintendencias. 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. Para las entidades sujetas a la aplicación del artículo 3. Regulación proporcional, las Superintendencias solicitarán la contratación de una auditoría externa de TI de conformidad con lo establecido en dicho artículo.

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.

Cuando las entidades y empresas supervisadas dispongan de sus componentes tecnológicos mediante el uso de servicios de computación en la nube proveídos por terceros, las Superintendencias podrán valorar la aceptación de informes de auditorías externas con las que ya cuenten dichos proveedores.

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, salvo en los casos en que se trate de proveedores de servicios de computación en la nube que ya cuentan con auditorías independientes.

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:

a) 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.
b) Las funciones para la evaluación de la gestión de riesgos de seguridad cibernética establecidas en los lineamientos generales del presente reglamento.
c) Componentes revelados en el perfil tecnológico de la entidad o empresa supervisada.
d) Entidades y empresas supervisadas, así como áreas de negocio y áreas de TI por considerar en cada proceso.
e) Proveedores de bienes y servicios de TI que, según los riesgos identificados, requieran la evaluación de una auditoría externa de TI, en cuyo caso, se evaluaran los procesos aplicables a la entidad o empresa supervisada y cualquier otro aspecto que esté relacionado con los bienes y servicios de TI tercerizados.
f) El periodo de cobertura.
g) 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 tres 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:

a) la copia del contrato suscrito por los servicios de auditoría, y
b) 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:

a) El informe de la auditoría externa de TI.

b) 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.
c) La matriz de evaluación del marco de gobierno y gestión de TI.
d) 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. Las acciones que se incluyan en el plan de acción deben establecerse en función del tamaño, complejidad y modelo de negocio, así como de los niveles de apetito, tolerancia y capacidad de riesgo establecidos.

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.

Las Superintendencias comunicaran a las entidades y empresas supervisadas, dentro del plazo de diez días hábiles contados a partir de recibida la solicitud de prórroga, la aceptación o rechazo de dicha solicitud. En caso de aceptación de la solicitud, se comunicará a la entidad o empresa supervisada el plazo adicional concedido. Dichas comunicaciones se realizarán 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:

a) 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.
b) 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 a fin de que se realicen los ajustes necesarios en los nuevos contratos y acuerdos de nivel de servicio.
En casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.

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:

a) Las sociedades corredoras de seguros deben implementar los procesos de su marco de gestión de TI gradualmente como máximo durante los primeros cuatro años contados a partir de la entrada en vigor del reglamento.

b) 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:

a) 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.

b) 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:

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

Disposición transitoria sexta. Perfil tecnológico

El contenido del perfil tecnológico y la guía para la descarga, llenado y remisión que deberán utilizar las entidades y empresas supervisadas serán los que se encuentran vigentes de conformidad con lo establecido en los lineamientos.

Las Superintendencias comunicarán a las entidades y empresas supervisadas la fecha a partir de la cual el contenido y la guía para descarga, llenado y remisión del perfil tecnológico incluirá las modificaciones reglamentarias.

Disposición transitoria séptima. Implementación de las modificaciones reglamentarias

Las entidades y empresas supervisadas deben validar que cumplan con las disposiciones de la presente modificación reglamentaria; cuando presenten brechas deberán elaborar planes de implementación para atender dichas brechas.

Las entidades y empresas supervisadas dispondrán de un plazo no mayor a tres años contados a partir de la fecha de publicación del presente reglamento en el diario oficial La Gaceta, para finalizar los planes de implementación.

Sin perjuicio de lo anterior, para la elaboración de los planes de implementación se deben considerar los plazos establecidos en los siguientes artículos de la modificación reglamentaria y en sus lineamientos

generales, a fin de que la ejecución de los planes permita el cumplimiento de los plazos establecidos en dichos artículos:

Artículo 39. Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias
Artículo 40. Comunicado de incidentes a los clientes
Artículo 41. Reporte histórico de incidentes
Artículo 45. Comunicación de cambios significativos del perfil tecnológico
Artículo 47. Alcance y plazo de la auditoría externa de TI
Artículo 48. Periodicidad de las auditorías externas de TI

Los planes de implementación deberán estar a disposición de las Superintendencias cuando estas lo requieran. Dichos planes podrán ser considerados para definir los alcances de la auditoría externa de TI o ser considerados como parte de la evaluación de las auditorías externas de TI.

Rige a partir de su publicación en el diario oficial La Gaceta."

Atentamente,

Documento suscrito mediante firma digital.

Celia Alpízar Paniagua
Secretaria interina del Consejo

Comunicado a: *Sistema financiero nacional, Asociación Costarricense de Auditores en Informática (c.a: Superintendencias, Intendencias y Auditoría Interna).*