Propuesta de modificación al Reglamento General de Gestión de la Tecnología de Información,
(Acuerdo CONASSIF 5-17)

MATRIZ DE OBSERVACIONES EXTERNAS
Versión 1

Acuerdo CONASSIF: CNS-1853/06 y CNS-1854/05, del 16 de abril de 2024.

Texto enviado a consulta	Observaciones y comentarios recibidos	Observaciones y comentarios Superintendencias	Texto modificado
Proyecto de acuerdo			**Proyecto de acuerdo**
"El Consejo Nacional de Supervisión del Sistema Financiero (Conassif).			"El Consejo Nacional de Supervisión del Sistema Financiero (Conassif).
considerando que:			**considerando que:**
consideraciones de orden legal y reglamentario	**[1]ABC** En términos generales se debe considerar lo siguiente: Se deberían incluir disposiciones sobre las obligaciones que asumen las superintendencias para proteger esa información, más allá de las regulaciones ya existentes y aplicables. Asimismo, la carga regulatoria del nuevo reglamento es considerable. Se recomienda valorar el impacto que ello tendrá en la innovación y la adopción de nuevas tecnologías, así como en las decisiones de inversión de las entidades, en esta materia.	**[1]No procede** Las disposiciones sobre las obligaciones que asumen las Superintendencias para proteger la información ya están definidas en la legislación aplicable a cada una de las superintendencias, así como en lo dispuesto en la Ley Orgánica del Banco Central de Costa Rica. Por otro lado, en términos generales, para abordar los temas de la carga regulatoria se incluyó la disposición transitoria séptima, que indica que cuando se presenten brechas se deberán elaborar planes de implementación para atender dichas brechas en un plazo no mayor a tres años contados a partir de la fecha de publicación del presente reglamento en el diario oficial La Gaceta.	**consideraciones de orden legal y reglamentario**

		Con relación a la adopción de nuevas tecnologías, así como en las decisiones de inversión de las entidades, en esta materia, como práctica general toda organización debería implementar controles compensatorios en función de los riesgos mientras se realizan los ajustes o incorporan los procesos de innovación, los cuales consideren las tecnologías emergentes, el conocimiento y los datos de la entidad. Es necesario que la adopción y uso de las tecnologías emergentes y la implementación de innovación en las entidades y empresas supervisadas sean incorporados dentro de la gestión de riesgos de cada entidad. En materia de regulación de TI no se trata de una regulación nueva, data ya desde la primera versión emitida en el 2009 y ha tenido varias actualizaciones. Este cambio busca un acercamiento al estándar Cobit y está alineado con las sanas prácticas de la materia; asimismo, está en línea con el grado de madurez de la industria, lo cual, se constató mediante un cuestionario enviado a las entidades supervisadas, lo cual, entre otros aspectos, permitió constatar que la mayoría de las entidades utilizan estándares de referencia para fines de gestión de TI.	
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			**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".			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.			**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.			**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,			**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.			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.			**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.			**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			**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.			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.			**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.			**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.			**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.			**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			**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:			**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.	**[2]COOPEFYL** Con relación al propósito a) del considerando XII, la integración de las normas regulatorias que aprueba los entes competentes en el país como es el caso de la SUGEF debe asegurar que las nuevas regulaciones se integren sin problemas con otras normativas vigentes para evitar conflictos o redundancias, como es el caso del Acuerdo SUGEF 25-23 de regulación proporcional que exime a un grupo de cooperativas de la aplicación del Gobierno Corporativos, Idoneidad y Administración de riesgos y crea un desbalance estableciendo un índice de suficiencia patrimonial del 16% para dicho grupo de CAC a partir de diciembre 2024. A la fecha, no se dispone por parte del ENTE REGULADOR de una justificación clara y transparente para tales decisiones, y más bien crea un desbalance en la protección contra los riesgos y la viabilidad operativa de las cooperativas que se encuentran bajo la normativa SUGEF 25-23, por lo que hay una incongruencia con la integralidad de los riesgos de la cooperativa.	**[2]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se	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.

		encuentra a disposición de las entidades. Por otra parte, el proyecto del Acuerdo SUGEF 25-23 tiene un marco considerativo que desarrolló todo el enfoque de proporcionalidad. Además, hay varias notas de respuesta dirigidas a Coopefyl mediante las cuales se le explica el enfoque de proporcionalidad, donde se expusieron los argumentos de la Superintendencia. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.			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			**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	**[3]COOPEFYL** Con relación considerando XIII, el acuerdo SUGEF 25-23 exime a algunas cooperativas de este requerimiento y por ello incrementa el	**[3]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo,	**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.	índice de suficiencia patrimonial al 16%, y en esta propuesta refuerza las responsabilidades del órgano de Dirección como parte del Gobierno Corporativo, no se comprende el desbalance en la norma vigente y la propuesta en consulta. Con relación considerando XIV, la SUGEF debería realizar un análisis que consideren cómo las nuevas normas interactúan con las existentes. Esto implica revisar la legislación actual para identificar cualquier posible sobreposición o contradicción con la nueva regulación propuesta. Acuerdo SUGEF 25-23 regulación proporcional para las cooperativas de ahorro y crédito.	idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se encuentra a disposición de las entidades. Por otra parte, el proyecto del Acuerdo SUGEF 25-23 tiene un marco considerativo que desarrolló todo el enfoque de proporcionalidad. Además, hay varias notas de respuesta dirigidas a Coopefyl mediante las cuales se le explica el	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.

		enfoque de proporcionalidad, donde se expusieron los argumentos de la Superintendencia. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.	**[4]ISACA** XIV. Debe utilizarse el término "Se espera", no se observa con esto la Directriz requerida. Debería indicarse de una vez XIV. Los miembros de los ... gerencia deben comprometerse a adaptar ...	**[4]Procede** Si bien no se adoptó el enfoque directamente, se mejora la redacción para reforzar el compromiso.	**XIV.** Se espera que los miembros de los Órganos de Dirección y de la Alta Gerencia se ~~vean~~ comprometan~~idos~~ 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			**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.	**[5]COOPEFYL** 1-Para hacer frente a este requerimiento es necesario disponer de la administración integral de riesgos en la organización, sin embargo, el Acuerdo 25-23 elimina dicho requerimiento y a su vez, compensan con un aumento en el índice de suficiencia patrimonial. 2-La cooperativa debe desarrollar estrategias de mitigación basadas en los resultados de las evaluaciones de riesgos, que pueden incluir tanto medidas técnicas como procedimientos administrativos por lo	**[5]No procede** 1-Se atendió en las observaciones 2 y 3. 2-Efectivamente, lo que se indica refleja la expectativa del supervisor.	**XV.** Para hacer frente a la naturaleza cambiante de las amenazas cibernéticas, es necesario ~~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.

	tanto es necesario disponer de estas evaluaciones de riesgos en forma regular que consideren tantas amenazas internas como externas, la probabilidad de ocurrencia y el impacto potencial en la organización.		
	[6]CB Es necesario incorporar además del DRP; un ciber recovery plan orientado al marco de respuesta de incidentes de ciberseguridad, recordando que en caso de delito informático el tema no es el tiempo de recuperación sino la supervivencia.	**[6]Procede (el comentario)** Lo que se indica en el comentario efectivamente está incorporado en la regulación; tanto el tema de la recuperación como la supervivencia están relacionados y consecuentemente el enfoque indicado en el comentario está incluido en la regulación. Las entidades deben diseñar los mecanismos de control alineados a estándares internacionales, buenas prácticas y marcos de referencia, que, de conformidad con su modelo de negocio y riesgos les permitan ser resilientes. En este sentido la entidades y empresas supervisadas a su discreción y en función de su modelo de negocio pueden diseñar los DRP separados o integrados.	
	[7]ISACA ... cibernéticas, es necesario que las entidades ...	**[7] Procede** Se ajusta para reforzar la idea contenida en la disposición del considerando.	
consideraciones sobre la gestión de la tecnología de información			**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	**[8]ISACA** XVI. El término adecuado es .... en caso de eventos tecnológicos	**[8]No procede** Desde la perspectiva del regulador el interés es utilizar el término "incidente" ya que hace referencia a aquello que tiene impacto negativo, sin embargo, la entidad puede darle un alcance mayor e incluir eventos.	**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.			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.	**[9]ISM** Si queremos que el cambio se dé, este reglamento ya debería referiste al diseño e implementación de un "Sistema de gobierno y gestión de TI" en las empresas. Las entidades supervisadas y los auditores tienen que comprender que lo que se construye es un Sistema único y personalizado en las organizaciones, que debe operar de forma natural y no como un mundo paralelo-documentado copia de COBIT.	**[9]No procede** Se prefiere el término de marco de gobierno y gestión de TI, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término marco está más alineado con los fines regulatorios, mientras que el término "sistema" se relaciona más con la implementación.	**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			**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.	**[10]ISACA** XVIII. Según reglas gramaticales usar ... eficiencia y conveniencia. Sin embargo, ...	**[10]Procede** Se ajusta la redacción.	**XVIII.** La migración a la nube brinda enormes oportunidades, eficiencia~~s~~ 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,	**[11]BCR** Se solicita detallar cuál es el contenido mínimo que se debe considerar, para el modelo de responsabilidades	**[11]No procede** El considerando no hace referencia a un "modelo de responsabilidades compartidas" en	**XIX.** Es importante que las entidades y empresas supervisadas tengan definida~~s~~ 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.	compartidas, así como en los controles administrativos y técnicos.	particular. El contenido es algo que corresponde definir a las partes involucradas de conformidad con el servicio adquirido.	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.
	[12]CB Se solicita detallar cuál es el contenido mínimo que se debe considerar, para el modelo de responsabilidades compartidas, así como en los controles administrativos y técnicos.	**[12]No procede** El considerando no hace referencia a un "modelo de responsabilidades compartidas" en particular. El contenido es algo que corresponde definir a las partes involucradas de conformidad con el servicio adquirido.	
	[13]ISACA XIX. ... tengan definidas las obligaciones ...	**[13]Procede** Se ajusta la redacción.	
consideraciones prudenciales sobre la tercerización de bienes y servicios de TI	**[14]QUÁLITAS** La aseguradora no puede hacerse responsable de estos servicios de los cuales son de tan alto nivel ya que no se tienen contacto con los proveedores.	**[14]No procede** Tal como se indica en el 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."	**consideraciones prudenciales sobre la tercerización de bienes y servicios de TI**
XX. Los proveedores de bienes y servicios son ampliamente utilizados para proporcionar servicios,			**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.			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.	**[15]COOPEFYL** Con relación a la consideración XXI: Lo que se debe incluir en los contratos tercerizados es suministro de la calidad del servicio y tiempos de atención, entre otros.	**[15]Procede (el comentario)** Lo sugerido en el comentario forma parte de lo que debe contemplar la entidad. Lo sugerido es una parte de lo que es importante contemplar por parte de la entidad y está incluido en el proyecto de modificación reglamentaria.	**XXI.** Los proveedores de bienes y servicios de TI y su cadena de suministro no están dentro del alcance de esta regulación~~.~~ ~~s~~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, a 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.
	[16]ISACA XXI. ... de esta regulación. Sin embargo, ... tercerizados; lo anterior, a través ...	**[16]Procede** Se ajusta la redacción.	
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	**[17]ISACA** XXII. ... y seguridad cibernética. Sin embargo, ...	**[17]Procede** Se ajusta la redacción.	**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~~.~~ ~~s~~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.			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			**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.	**[18]COOPEFYL** Con relación al considerando XXIII: La importancia de la administración de los riesgos en el tema de TI, y que hace necesario su atención por parte de las organizaciones y que es contradictorio con eximir del Acuerdo Sugef 2-10 a las cooperativas de regulación proporcional.	**[18]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace	**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.

		referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.			**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.			**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.			**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	**[19]ISACA** XXVII. ... las entidades y empresas supervisadas sobre los elementos mínimos ... (para mantener consistencia con el apartado XXVIII)	**[19]No procede** La redacción incorporada en el considerando es clara.	**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.			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.			**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			**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.			**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.	**[20]ISACA** Ya que el marco regulatorio está orientado al Marco de Referencia Cobit, debería también considerarse que el auditor externo cuente con la acreditación en fundamentos de cobit 2019. También es importante considerar que los fiscalizadores de TI de las entidades supervisores cuenten también tanto con CISA como Fundamentos Cobit. Esto con el fin de que se puedan dar opiniones entre profesionales homólogos.	**[20]Procede** El principal requisito para los auditores externos de TI es la certificación CISA de ISACA, la cual, a su vez, requiere formación y capacitación continua de los profesionales acreditados. En relación con el requerimiento de CISA para los supervisores, es algo que las Superintendencias valorarán respecto a los perfiles de los supervisores.	**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			**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			**XXXI.** El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt~~ICITT~~) 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.			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.			**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.	**[21]QUÁLITAS** Los cambios de Cobit 5 a Cobit 2019 son significativos por los cual podría llevar a la empresa a gastos y horas hombre. Evaluar, Dirigir y Supervisar (EDS): En COBIT 5, este proceso se enfoca en evaluar la dirección y supervisión del gobierno de TI. En COBIT 2019, se expande para incluirla evaluación de la dirección, supervisión y evaluación del gobierno de la empresa. Alinear, Planificar y Organizar (APO): En COBIT 5, este proceso se centra en alinear la estrategia y los objetivos de TI con los de la empresa. En COBIT 2019, este proceso se amplía para incluir la alineación, planificación y organización del gobierno de la empresa. Construir, Adquirir e Implementar (BAI): En ambas versiones, este proceso se enfoca en la entrega y gestión de soluciones de TI.	**[21]No procede** En materia de regulación de TI no se trata de una regulación nueva, data ya desde la primera versión emitida en el 2009 y ha tenido varias actualizaciones. Este cambio busca un acercamiento al estándar Cobit y está alineado con las sanas prácticas de la materia; asimismo, está en línea con el grado de madurez de la industria, lo cual se constató mediante un cuestionario enviado a las entidades supervisadas, los cual, entre otros aspectos, permitió constatar que la mayoría de las entidades utilizan estándares de referencia para fines de gestión de TI. Para el cierre de las brechas que pueda tener la entidad en relación con las disposiciones del presente reglamento, se incluyó un transitorio séptimo.	**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.

	Entregar, Servir y Soportar (DSS): Se centra en la entrega y soporte de servicios de TI en ambas versiones. Monitorear, Evaluar y Valorar (MEA): En ambas versiones, se enfoca en la evaluación del desempeño y la conformidad para garantizar que se alcancen los objetivos de gobierno de TI.		
	[22]BNCR Para el inciso XXXIII Es importante que en el Reglamento se deje claro bajo qué mejor práctica va a evaluar el Regulador, ya que en algunos artículos define a COBIT2019 como mejor práctica y en otros apartados indica que se pueden adoptar las mejores prácticas de la industria, sin que quede claro a qué se refiere puntualmente. Por otra parte, las auditorías externas se basan en COBIT, y sería importante que haya total claridad en ese sentido. Es claro que las entidades deben analizar y adoptar las mejores prácticas que le permita mitigar sus riesgos, pero también es necesario que haya total claridad de las aspiraciones del Regulador.	**[22]No procede** Las expectativas de lo que solicita el regulador en materia de TI es lo que está contenido en este reglamento. Lo que el supervisor va a ver es la consistencia entre el perfil de TI de la entidad y la calidad de la gestión. La entidad es la que definirá el cómo implementa lo que se establece en el reglamento.	
	[23]CB Es importante que en el Reglamento se deje claro bajo qué mejor práctica va a evaluar el Regulador, ya que en algunos artículos define a COBIT 2019 como mejor práctica y en otros apartados indica que se pueden adoptar las mejores prácticas de la industria, sin que quede claro a qué se refiere puntualmente. Por otra parte, las auditorías externas se basan en COBIT, y sería importante que haya total claridad en ese sentido.	**[23]No procede** Las expectativas de lo que solicita el regulador en materia de TI es lo que está contenido en este reglamento. Lo que el supervisor va a ver es la consistencia entre el perfil de TI de la entidad y la calidad de la gestión. La entidad es la que definirá el cómo implementa lo que se establece en el reglamento.	

	Es claro que las entidades deben analizar y adoptar las mejores prácticas que le permita mitigar sus riesgos, pero también es necesario que haya total claridad de las valoraciones del Regulador.		
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.			**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.	**[24]ISACA** XXXV. Como parte de su objetivo, es que la regulación oriente a las entidades en el uso de estándares....	**[24]No procede** El considerando hace referencia a que 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 el reglamento.	**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			**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	**[25]OPCCCSS** La regulación dispuesta en materia de ciberseguridad sí aumenta los costos tanto de regulación como de gestión de los entes fiscalizados, por ende no se puede aseverar que no existe un impacto pues los requisitos a cumplir son mayores.	**[25]No procede** Debe aclararse que el contexto al que se refiere la Ley 8220 es a trámites y requisitos que deba cumplir el administrado ante la administración. El ámbito de esta regulación es prudencial; la Ley	**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.	Sumado que se aumentan las responsabilidades de estar supervisando los contratos de los proveedores y la atención de las funciones propias de cada puesto.	8220 no alcanza la regulación de tipo prudencial. Este impacto está en función de los trámites y requerimientos que genere el reglamento, no está en función de los alcances de supervisión.	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			**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.	**[26]COOPEFYL** El acuerdo Sugef 25-23 exime a un grupo de cooperativas de la administración de riesgos, temas críticos en cualquier organización con lo cual es indispensable desarrollarlos, sin embargo, la SUGEF debe revisar el castigo asignado de aumentar el índice de suficiencia patrimonial al 16%, ya que las cooperativas en el acuerdo deben continuar con la aplicación de la administración de riesgo, es innato a la gestión de cualquier organización, y mucho menos recibir un castigo tan alto al ISP del 16%.	**[26]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio.	**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.

		Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
	[27]COOPEALIANZA Se solicita modificar el nombre del reglamento al siguiente: REGLAMENTO DE GOBIERNO Y GESTIÓN EMPRESARIAL PARA LA INFORMACIÓN Y LA TECNOLOGIA, al estar basado este reglamento en el marco de buenas prácticas empresariales COBIT, es sabido que este cubre no sólo procesos de Tecnología, sino que además hay un alto porcentaje de los procesos que involucran procesos de negocio y procesos de soporte al negocio.	**[27] No procede** La propuesta de modificación reglamentaria toma como base diferentes estándares internacionales, mejores prácticas y marcos de referencia; no uno solo en particular.	
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.	**[28]COOPEFYL** El acuerdo Sugef 25-23 exime a un grupo de cooperativas de la administración de riesgos, temas críticos en cualquier organización con lo cual es indispensable desarrollarlos, sin embargo, la SUGEF debe revisar el castigo asignado de aumentar el índice de suficiencia patrimonial al 16%.	**[28]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas	**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.

		disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.			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:			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].			"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:			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**			"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].			**funcionario de hecho** […]". [Lo resaltado no es del original].
Ahora bien, la Procuraduría concluye que:			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].			"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:			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.	**[29]ISACA** a) ... teniendo en cuenta también el alto grado de interconexión ... / d) ... así como la continuidad del proceso de supervisión. / e) puede provocar un impacto estratégico negativo en las entidades super...	**[29]No procede** La redacción incorporada en el considerando es clara.	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.	**[30]SAGICOR** En cuanto al punto b. Gestión diligente de la relación con proveedores de bienes y servicios de TI. La gestión diligente de los proveedores de NEGOCIO (no de TI) que intercambien información crítica, no queda claro sobre cual órgano recae la responsabilidad, ya que los artículos 8, 9, 10 y 11, no lo aclaran. Gracias.	**[30]No procede** En los marcos de regulación vigente sobre gestión de riesgos de cada Superintendencia se hace referencia a gestión de riesgos operacionales. Por ejemplo, en el caso del Acuerdo SUGEF 2-10, respecto a riesgo operativo, se hace referencia de los riesgos de	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.

		tercerización de una forma general.	
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.			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.			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.			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.			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.			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:			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:			"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].			´ ... 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:			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			**"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.**			**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.			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].			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			**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.			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. No obstante, debido a los cambios y mejoras incorporados en la propuesta de modificación reglamentaria a partir de los resultados del proceso de consulta, el Consejo consideró conveniente enviarla nuevamente en consulta al medio, por lo que, mediante artículos 6 y 5 de las actas de las sesiones 1853-2024 y 1854-2024, celebradas el 16 de abril del 2024, el Conassif dispuso el envío en consulta de la citada propuesta de modificación reglamentaria en una segunda instancia durante un plazo de diez días hábiles; se recibieron comentarios y observaciones, los cuales, fueron evaluados y en lo pertinente fueron incorporadas al texto de la modificación reglamentaria.
dispuso:			**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:			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			**'REGLAMENTO GENERAL DE GOBIERNO Y GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN**
ACUERDO CONASSIF 5-24			**ACUERDO CONASSIF 5-24**
CAPÍTULO I			**CAPÍTULO I**
DISPOSICIONES GENERALES			**DISPOSICIONES GENERALES**
Artículo 1. Objeto			**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.			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.	**[31]COOPEFYL** ¿El acuerdo Sugef 25-23 exime de la administración de riesgos a las cooperativas reguladas proporcionalmente, como se manejará esta situación por la SUGEF que ahora	**[31]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de	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.

	manifiesta que por sanas prácticas debería desarrollarse? Sin embargo, como lo menciona la misma SUGEF en el Acuerdo Sugef 25-23 eximir de normativa hizo que aumentara el requerimiento cuantitativo en el ISP. Para las cooperativas de ahorro y crédito reguladas proporcionalmente están eximidas del Acuerdo CONASSIF 4-16 según el Acuerdo SUGEF 25-23, por lo tanto, la SUGEF ha creado un vació o indefiniciones no saludables en las normas para la regulación proporcional y además a castigado a las cooperativas con un ISP más alto16%, incluso superior al Indicador de Suficiencia Patrimonial los ENTES SISTÉMICOS SUPERVISADOS.	riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se encuentra a disposición de las entidades. Por otra parte, el proyecto del Acuerdo SUGEF 25-23 tiene un marco considerativo que desarrolló todo el enfoque de proporcionalidad. Además, hay varias notas de respuesta dirigidas a Coopefyl mediante las cuales se le explica el enfoque de proporcionalidad,	

		donde se expusieron los argumentos de la Superintendencia. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
Artículo 2. Alcance			**Artículo 2. Alcance**
Las disposiciones establecidas en este reglamento son de aplicación para:			Las disposiciones establecidas en este reglamento son de aplicación para:
a) Supervisados por SUGEF:			a) Supervisados por SUGEF:
1. Bancos comerciales del Estado			1. Bancos comerciales del Estado
2. Bancos creados por ley especial			2. Bancos creados por ley especial
3. Bancos privados			3. Bancos privados
4. Empresas financieras no bancarias			4. Empresas financieras no bancarias
5. Organizaciones cooperativas de ahorro y crédito			5. Organizaciones cooperativas de ahorro y crédito
6. Mutuales de ahorro y préstamo			6. Mutuales de ahorro y préstamo
7. Caja de Ahorro y Préstamos de la ANDE			7. Caja de Ahorro y Préstamos de la ANDE
b) Supervisados por SUGEVAL:			b) Supervisados por SUGEVAL:
1. Puestos de bolsa y sociedades administradoras de fondos de inversión			1. Puestos de bolsa y sociedades administradoras de fondos de inversión
2. Bolsas de valores			2. Bolsas de valores
3. Sociedades de compensación y liquidación			3. Sociedades de compensación y liquidación
4. Proveedores de precio			4. Proveedores de precio
5. Entidades que brindan servicios de custodia			5. Entidades que brindan servicios de custodia
6. Centrales de valores			6. Centrales de valores
7. Sociedades titularizadoras y fiduciarias			7. Sociedades titularizadoras y fiduciarias

8. Entidades de registros centralizados de letras de cambio y pagarés electrónicos			8. Entidades de registros centralizados de letras de cambio y pagarés electrónicos
c) Supervisados por SUGESE:			c) Supervisados por SUGESE:
1. Entidades aseguradoras y reaseguradoras			1. Entidades aseguradoras y reaseguradoras
2. Sucursales de entidades aseguradoras extranjeras			2. Sucursales de entidades aseguradoras extranjeras
3. Sociedades corredoras de seguros			3. Sociedades corredoras de seguros
d) Supervisados por SUPEN:			d) Supervisados por SUPEN:
1. Operadoras de pensiones complementarias			1. Operadoras de pensiones complementarias
2. Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social			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			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.			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.			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.	**[32]BPDC** Inciso e) Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados. ¿El alcance va dirigido a aquellos conglomerados que tienen	**[32]No procede** Para efectos de atender lo indicado en la observación, las entidades deben considerar lo que establece el artículo 141) Constitución de grupos y conglomerados	e) Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados.

	por ejemplo una empresa que es proveedora de servicios de TI? De ser así, se excluyen las empresas del conglomerado que no tengan que ver con el sector financiero	financieros, del Reglamento sobre Supervisión Consolidada, Acuerdo Conassif 16-22, el cual, establece lo siguiente: "El CONASSIF definirá, mediante reglamento, otras entidades o empresas nacionales o extranjeras, dedicadas a la actividad financiera, que podrán formar parte del grupo, tales como aquellas que apoyan la actividad del grupo financiero o las que, resultado de la valoración de riesgos por parte del supervisor responsable, evidencie que es necesario que sean parte del grupo para una mejor representación de las características particulares del modelo de negocio del grupo financiero resultante". Además, el Acuerdo Conassif 16-22, indica en las definiciones que, una empresa supervisada es aquella: empresa local o extranjera, integrante de un grupo o conglomerado financiero, incluida la empresa controladora, que por la naturaleza de sus actividades no esté sujeta a un régimen jurídico especial de supervisión a nivel local.	
Artículo 3. Regulación Proporcional			**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:	**[33]COOPEFYL** Para atender este tema, es necesario las metodologías de la administración de riesgos por lo tanto dejar de aplicar el Acuerdo Sugef 2-10 es impensable tal como lo establece el Acuerdo 25-23 de regulación Proporcional. De acuerdo con Basilea el enfoque con base a riesgos el sujeto obligado es	**[33]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia.	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:

	responsable de la gestión integral de riesgos de su negocio, sin embargo en el acuerdo SUGEF 25-23 de regulación proporcional la SUGEF exime a las cooperativas de ahorro y crédito de aplicar el acuerdo SUGEF 2-10 Reglamento sobre la Administración Integral de Riesgos, por lo tanto, se genera una imposibilidad material de abordar riesgos particulares como este caso de TI cuando no se aplica una integralidad a nivel de la organización.	Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
	[34]CB Se sugiere que este artículo se modifique en el sentido de que, mediante un estudio de aplicabilidad de este reglamento y el marco de gestión de TI a partir del tamaño, complejidad y modelo de negocio, debería permitirse a cualquier entidad definir la aplicación proporcional de	**[34]No procede** Las disposiciones contenidas en presente modificación reglamentaria contienen las expectativas de alto nivel esperadas por las Superintendencias, las cuales definen los aspectos más relevantes que se espera que las	

	este Reglamento conforme su contexto de riesgo, definiendo el nivel de profundidad requerido.	entidades y empresas supervisadas deban atender.	
	[35]ISACA 1. Se trata muy levemente el tema específico de análisis de riesgos (entiendo que lo visualizan como gestión de riesgos en forma general). 2.No se habla de realizar un BIA (puede ser que se asuma como parte de la gestión de riesgos) no se habla de las métricas necesarias a implementar. 3- No se habla de privacidad o información privada. 4. Considerar como requerimiento del auditor externo, la acreditación al menos en fundamentos de Cobit. b) No se obtuvo el anexo 2 para entender mejor cuál es ese alcance de evaluación.	**[35]No procede** 1-No se incluyen aspectos específicos relacionados con los riesgos ya que, la presente modificación regulatoria 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. 2- Se espera que las entidades y empresas supervisadas implementen los BIA como parte de las actividades de continuidad del negocio según lo establecen las mejores prácticas, estándares internacionales y marcos de referencia. Por otra parte, el reglamento indica que las entidades pueden implementar las mejores prácticas, estándares y marcos de referencia más acordes a su modelo de negocio y perfil de riesgos, en este sentido las entidades podrían implementar la norma ISO 22317, la cual, es una especificación técnica que proporciona orientación detallada sobre cómo establecer, implementar y mantener un proceso de Análisis de Impacto en el Negocio (BIA, por sus siglas en inglés), o cualquier otra.	

		3- Con relación a la privacidad y protección de los datos, en Costa Rica ya existe legislación específica, la Ley 8968, Ley de protección de la persona frente al tratamiento de sus datos personales, la cual, es una normativa que tiene como objetivo garantizar la privacidad y la seguridad de la información personal de los individuos. Esta ley establece las obligaciones que deben cumplir las organizaciones que recopilan, almacenan o procesan datos personales, así como los derechos que tienen las personas sobre sus datos. 4-El principal requisito para los auditores externos de TI es la certificación CISA de ISACA, la cual, a su vez, requiere formación y capacitación continua de los profesionales acreditados. Adicionalmente, las matrices de evaluación se ajustaron para aclarar que la revisión no es un check list, sino que se debe realizar en función del modelo de negocio y sus riesgos.	
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.			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,			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.			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.	**[36]ISTMO** Con relación al artículo 33 evaluar dejarlo como obligatorio, lo anterior fundamentado en lo siguiente: a) Los intermediarios de seguros manejan una gran cantidad de información de los asegurados b) No es un punto que sea considerado oneroso, hoy en día existen mecanismos y herramientas incluso open source con las cuales pueden llevar a cabo esta tarea y conocer de forma clara las vulnerabilidades a las que están expuestas. Incluso en Costa Rica se pueden suscribir a fuentes oficiales sin ningún costo para recibir notificaciones de las vulnerabilidades más importantes. c) Todos los días salen nuevas vulnerabilidades por lo que no tener conocimiento y visibilidad de las mismas constituyen un riesgo alto.	**[36] No procede** Si bien los programas de análisis de vulnerabilidades y pruebas son cruciales para la mayoría de las organizaciones, su necesidad y escala pueden ser menores en las Sociedades Corredoras de Seguros, debido a factores como la menor complejidad de infraestructura, recursos limitados y el enfoque en medidas proporcionales. Por otra parte, este es un aspecto que puede ser calibrado mediante la práctica supervisora y así generar ajustes cuando sea necesario.	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).			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:			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			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.			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.			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			**Artículo 4. Definiciones y abreviaturas**
Para efectos de este reglamento y sus lineamientos generales, se utilizan las siguientes definiciones y abreviaturas:	**[37]CAJAANDE** Se recomienda incluir la definición de tecnología emergente para una mejor interpretación de la norma.	**[37] No procede** En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria.	Para efectos de este reglamento y sus lineamientos generales, se utilizan las siguientes definiciones y abreviaturas:
	[38]BNCR Se considera relevante que en el artículo 4 se adicione la definición de "Incidente de seguridad de información, activo de información, Ciberseguridad", con el fin de homologar el concepto para todas las partes.	**[38]No procede** La propuesta de modificación regulatoria ya incluye una definición de "seguridad cibernética". En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información, y considera propias las definiciones incluidas en los reglamentos aprobados por el CONASSIF, así mismo algunas están descripciones están detalladas en los lineamientos generales. Adicionalmente, en la sección II del Capítulo VI, se aclaran los aspectos relacionados con la gestión de los incidentes de	

		seguridad cibernética relacionados con la entidad o empresa supervisada. Además, las entidades y empresas supervisadas, de conformidad con el estándar, mejor práctica o el marco de referencia implementado, deberán adoptar y adaptar lo indicado en las definiciones como parte del desarrollo de los controles administrativos. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria.	
	[39]OPCCCSS Se hace referencia a nuevos conceptos como vectores de ataque, defensa en profundidad, computación en la nube, datos en reposo, confianza cero, necesidad del mínimo conocimiento, metas de sustentabilidad, metas de integridad, ciclos del negocio, gobernanza y ecosistema, etc., por lo cual se recomienda incluir la definición de cada uno para eliminar todo tipo de ambigüedad.	**[39] No procede** En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria.	
	[40]ABC Resulta conveniente adicionar la definición de los términos “Incidente de seguridad de información”, “activo de información” y “Ciberseguridad”.	**[40]No procede** La propuesta de modificación regulatoria ya incluye una definición de “seguridad cibernética”. En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información, y considera propias las definiciones incluidas en los reglamentos aprobados por el	

		CONASSIF, así mismo algunas están descripciones están detalladas en los lineamientos generales. Adicionalmente, en la sección II del Capítulo VI, se aclaran los aspectos relacionados con la gestión de los incidentes de seguridad cibernética relacionados con la entidad o empresa supervisada. Además, las entidades y empresas supervisadas, de conformidad con el estándar, mejor práctica o el marco de referencia implementado, deberán adoptar y adaptar lo indicado en las definiciones como parte del desarrollo de los controles administrativos. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria.	
	[41]CB Se considera relevante que en el artículo 4 se adicione la definición de "Incidente de seguridad de información, activo de información, Ciberseguridad", con el fin de homologar el concepto para todas las partes.	**[41]No procede** La propuesta de modificación regulatoria ya incluye una definición de "seguridad cibernética". En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información, y considera propias las definiciones incluidas en los reglamentos aprobados por el CONASSIF, así mismo algunas están descripciones están detalladas en los lineamientos generales.	

		Adicionalmente, en la sección II del Capítulo VI, se aclaran los aspectos relacionados con la gestión de los incidentes de seguridad cibernética relacionados con la entidad o empresa supervisada. Además, las entidades y empresas supervisadas, de conformidad con el estándar, mejor práctica o el marco de referencia implementado, deberán adoptar y adaptar lo indicado en las definiciones como parte del desarrollo de los controles administrativos. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria.	
	[42]ISM Sistema de gobierno y gestión de TI: sistema holístico empresarial para el gobierno y la gestión de las tecnologías de información, conformado por un conjunto de componentes como procesos, estructuras, personas, herramientas, entre otros, creado a partir de un marco de gobierno y gestión de TI base.	**[42]No procede** La redacción incorporada en la definición y el contenido son claros. Se prefiere el término de “marco de gobierno y gestión de TI”, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término “marco” está más	

		alineado con los fines regulatorios, mientras que el término “sistema” se relaciona más con la implementación.	
	[43]BAC Se solicita incluir en el glosario la definición de arquitectura organizacional, la definición de tecnologías emergentes y definición de arquitectura de negocio.	**[43]No procede** En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información, y considera propias las definiciones incluidas en los reglamentos aprobados por el CONASSIF, así mismo algunas están descripciones están detalladas en los lineamientos generales. Además, las entidades y empresas supervisadas, de conformidad con el estándar, mejor práctica o el marco de referencia implementado, deberán adoptar y adaptar lo indicado en las definiciones como parte del desarrollo de los controles administrativos. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria.	
	[44]MUCAP Se considera relevante aclarar si en la definición de “Bienes y servicios de TI críticos” y "Procesos críticos", lo referente al “Impacto significativo” es determinado a criterio de cada entidad. Adicionalmente, en la definición de "Proveedores de bienes y servicios de TI críticos" está indicados en términos de cualquier persona física o jurídica que ofrece servicios de T.I., para lo	**[44] No procede** El inciso j) del artículo 4; define lo que son “procesos críticos”. Para determinar el impacto y la criticidad a nivel de proceso, bien o servicio, las entidades y empresas supervisadas pueden realizar análisis de impacto de conformidad con diferentes técnicas dispuestas en las mejores prácticas, estándares	

	cual se considera relevante ampliar esta definición de manera tal que se considere el criterio por el cual se consideran críticos. Por otra parte, en la definición "Resiliencia operativa digital", los mecanismos alternos de trabajo no basados en tecnología, razón por la cual con esta definición no queda claro si serán siempre válidos en la gestión de la continuidad del negocio	internacionales y marcos de referencia aplicables a la industria de las TI. En el artículo 26, se indica deben mantener identificados sus proveedores de bienes y servicios de TI críticos, a través de un análisis de riesgos.	
	[45]ISACA Deberían considerar términos asociados a la privacidad de datos	**[45] No procede** En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son de uso común en la industria de las tecnologías de la información. Las definiciones de uso común se pueden consultar en documentos técnicos referentes de la industria. Ya existe la Ley 8968. Esta ley establece las obligaciones que deben cumplir las organizaciones que recopilan, almacenan o procesan datos personales, así como los derechos que tienen las personas sobre sus datos; la propuesta de reglamento considera los aspectos inmersos en la citada ley.	
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.			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			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.			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.			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.			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.			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).			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.			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.			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.			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			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.			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).	**[46]ISTMO** En la definición: 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). Se propone dejar bien claro y delimitado si se incluyen o no se incluyen proveedores de servicios de negocio que manejen información considerada sensible, lo anterior se fundamenta que en varios artículos hacen referencia a Proveedores de Bienes y Servicios de TI, únicamente TI, dejando una gran duda y área gris porque en los artículos 11, 21 (detallados en los lineamientos generales), 25, 27 y 47 se hace referencia en algunos a proveedores de TI y en otros habla de servicios	**[46]Procede** Indistintamente si se trata o no de un proveedor de bienes y servicios de TI críticos o de negocio, la entidad debe gestionar los riesgos. En las disposiciones reglamentarias, cuando no se incluye el acrónimo "TI", entonces se hace referencia al negocio. Se ajustó la redacción de la definición. Lo indicado en la observación sobre incluir o no proveedores de servicios de negocio que manejen información considerada sensible, dependerá de si a estos la entidad le delegó un proceso crítico o si estos apoyan un proceso crítico. Se aclaró el alcance de la definición k. Finalmente, El artículo 25 sobre responsabilidades de la tercerización incluye: "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".	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, los cuales apoyan los procesos críticos indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).
l) **Resiliencia operativa digital**: Capacidad de una entidad o empresa supervisada para mantener la			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.			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.	**[47]COOPEALIANZA** Sobre la definición del punto m) Seguridad cibernética: Se solicita utilizar únicamente el concepto de Seguridad de Información, gestionar dos conceptos confunde a las partes interesadas; la seguridad de la información ya considera la gestión del riesgo desde la perspectiva de la información en cuanto a sus atributos de disponibilidad, confidencialidad e integridad; es decir cubre los riesgos que impactan el ámbito de Internet.	**[47] No procede** La propuesta reglamentaria contiene las expectativas de alto nivel que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Por lo que, para las Superintendencias es relevante destacar el tema de la seguridad cibernética. Sin embargo, se eliminó lo referente al deber de establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	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.	**[48]BPDC** Se sugiere incluir en la definición de Seguridad de la Información, que protege los datos indistintamente de sus formato físico, digital y contenido y cambiar Seguridad Cibernética por "Ciberseguridad" dado que es un término más conocido en la industria	**[48] No procede** Seguridad Cibernética y Ciberseguridad se utilizan de forma indistinta, para efectos del presente Reglamento se utiliza seguridad cibernética.	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.
	[49]COOPEALIANZA Sobre la definición del punto n) Seguridad de la información: Se solicita utilizar la siguiente redacción en línea con el punto anterior: n) Seguridad de la información: Práctica de gestionar los riesgos que afectan los objetivos de confidencialidad, integridad y	**[49]No procede** La redacción incorporada en la definición y el contenido son claros. Las definiciones de uso poco común se pueden consultar en documentos técnicos referentes de la industria.	

	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 que son provistos por la entidad en sus propias instalaciones, desde proveedores de bienes y servicios de TI críticos desde sus instalaciones locales y/o desde Internet.		
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.			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.			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.			Este reglamento incorpora como propias las demás definiciones dispuestas en la reglamentación vigente aprobada por el CONASSIF.
Artículo 5. Lineamientos generales			**Artículo 5. Lineamientos generales**
Los superintendentes podrán emitir, conjuntamente, los lineamientos generales que consideren necesarios para la aplicación de este reglamento.			Los superintendentes podrán emitir, conjuntamente, los lineamientos generales que consideren necesarios para la aplicación de este reglamento.
CAPÍTULO II			**CAPÍTULO II**
GOBIERNO Y GESTIÓN DE TI			**GOBIERNO Y GESTIÓN DE TI**
Sección I. Marco de gobierno y gestión de TI			**Sección I. Marco de gobierno y gestión de TI**
Artículo 6. 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.	**[50]COOPEFYL** Según el artículo 3 de este reglamento Coopefyl esta eximido por lo tanto la discrecionalidad no cabe porque en la SUGEF 25-23 indican lo contrario y nos aumentaron el indicador de la Suficiencia Patrimonial, por lo que en	**[50] No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de	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.

	este caso deberían bajar el indicador de Suficiencia Patrimonial. Sin embargo, en los lineamientos generales en el anexo 2 Procesos de evaluación de la gestión de TI para la regulación proporcional se deben cumplir 13 procesos y uno de -ellos están referido a la Gestión de Riesgos, con lo cual no hay congruencia con lo definido en este artículo y el acuerdo SUGEF 25-23, de eximir a estas cooperativas de la aplicación según SUGEF 25-23.	supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se encuentra a disposición de las entidades. Por otra parte, el proyecto del Acuerdo SUGEF 25-23 tiene un marco considerativo que desarrolló todo el enfoque de proporcionalidad. Además, hay varias notas de respuesta dirigidas a Coopefyl mediante las cuales se le explica el enfoque de proporcionalidad, donde se expusieron los	

		argumentos de la Superintendencia. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos. Por otra parte, el "Artículo 3 Regulación Proporcional", indica entre otros aspectos que 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 deberá incluir para efectos del alcance de la auditoría externa de TI, al menos, los procesos de evaluación que se especifican en el anexo 2 de los lineamientos generales del reglamento**.**	
	[51]COOPEALIANZA Se indica que la entidad debe de diseñar, implementar, controlar y mantener un marco de gobierno y gestión de TI, sin embargo, el presente reglamento solicita a la auditoría externa evaluar y cumplir la matriz de evaluación con la totalidad de los procesos y para cada proceso la totalidad de prácticas establecidas en el Cobit 2019,por ende no se le permite	**[51]No procede** Tal como se indica en la propuesta de modificación reglamentaria, la entidad debe diseñar, implementar, controlar y mantener un marco de gobierno y gestión de TI. Efectivamente, la propuesta de modificación reglamentaria solicita a la auditoría externa evaluar y cumplir la matriz de evaluación; sin embargo, cabe	

	a la entidad diseñar la metodología de acuerdo a su estrategia organizacional, el apetito, la tolerancia y la capacidad de riesgo, tamaño, complejidad, modelo de negocio y las políticas aprobadas por el Órgano de Dirección. Consideramos que existe una contradicción que se viene presentando desde el reglamento anterior; ya que se indica que se podrá utilizar otros estándares internacionales, mejores prácticas y marcos de referencia pero que sin embargo es conocido que la SUGEF define las reglas por medio de la matriz de evaluación y no deja claridad de la posibilidad de crear una propia matriz de evaluación o bien alinearse a los niveles de capacidad que propone COBIT 2019 donde hasta un nivel 2 podría definirse como Mejorable, hasta un nivel 3 como Aceptable y por encima de nivel 3 como Fuerte.	destacar, que con la presente propuesta de modificación regulatoria, a su vez, se actualizó la matriz de evaluación, en la cual, las entidades deberán seleccionar los procesos y para cada proceso las prácticas que le apliquen de conformidad con su estrategia organizacional, el apetito, la tolerancia y la capacidad de riesgo, tamaño, complejidad, modelo de negocio y las políticas aprobadas por el Órgano de Dirección. También, se destaca que no existe una contradicción al utilizar otros estándares internacionales, mejores prácticas y marcos de referencia, ya que los criterios de evaluación están dispuestos en la matriz de evaluación y esta a su vez, está alineada a la última versión de Cobit y, concomitantemente, al ser este un marco de referencia cuyo diseño incluye un apartado denominado "Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)" y la Referencia específica; las entidades y empresas supervisadas podrían implementar estas, manteniendo los elementos mínimos requeridos en función de su estrategia organizacional, el apetito, la tolerancia y la capacidad de riesgo, tamaño, complejidad, modelo de negocio y las políticas aprobadas por el Órgano de Dirección. En virtud de lo anterior, la matriz contendrá los elementos mínimos de control, indistintamente del estándar, marco de referencia o	

		mejor práctica implementada por la entidad o empresa supervisada. Por su parte, para el cierre de las brechas que pueda tener la entidad en relación con las disposiciones del presente reglamento, se incluyó un transitorio séptimo. Además, se aclara que, las entidades y empresas supervisadas no deberán crear una propia matriz de evaluación, ya que, las Superintendencias la pondrán a disposición. Finalmente, queda a discreción de las entidades y empresas supervisadas, de conformidad con el análisis de brechas, utilizar o alinearse a los niveles de capacidad que propone COBIT 2019 donde hasta un nivel 2 podría definirse como Mejorable, hasta un nivel 3 como Aceptable y por encima de nivel 3 como Fuerte; ya que las Superintendencias no requieren la implementación de prácticas utilizando dichos modelos, sino que están basadas en de su estrategia organizacional, el apetito, la tolerancia y la capacidad de riesgo, tamaño, complejidad, modelo de negocio y las políticas aprobadas por el Órgano de Dirección.	
	[52]BNCR Se considera importante que se deje claro, en este artículo, si el alcance del Marco de Gobierno de TI, en el caso de las entidades miembros de un conglomerado, aplica en su totalidad o por integrante del conglomerado.	**[52] Procede** Lo indicado por la entidad está claramente establecido en la norma. En el artículo 16, se establece que, en caso de que los grupos y conglomerados financieros tipifiquen su gestión de TI como	

	Lo anterior, puede complementarse con lo consignado en el artículo 16 del presente reglamento.	corporativa, 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.	
	[53]ABC La norma hace referencia al marco de gobierno corporativo de TI de las entidades y empresas supervisadas; no obstante, por la redacción no resulta claro si el alcance de este debe ser por entidad o si puede ser corporativo.	**[53] Procede** Lo indicado por la entidad está claramente establecido en la norma. En el artículo 16, se establece que, en caso de que los grupos y conglomerados financieros tipifiquen su gestión de TI como corporativa, 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.	
	[54]CB Se considera importante que se deje claro en este artículo, si el alcance del Marco de Gobierno de TI en el caso de las entidades miembros de un Conglomerado aplica en su totalidad o por integrante del conglomerado. Lo anterior, puede complementarse con lo consignado en el artículo 16 del presente Reglamento.	**[54] Procede** Lo indicado por la entidad está claramente establecido en la norma. En el artículo 16, se establece que, en caso de que los grupos y conglomerados financieros tipifiquen su gestión de TI como corporativa, 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.	
	[55]ISM Las entidades y empresas supervisadas deben diseñar, implementar, controlar y mantener un Sistema 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. --- "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". Aquí no debe diferenciarse las unidades de TI de las áreas de Negocio, el sistema es para la empresa y es necesario que interactúen todas las estructuras requeridas; puede haber componentes del sistema externalizados, pero finalmente el sistema es de la empresa.	**[55]No procede** El término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación. Al referirse en la propuesta de modificación reglamentaria a las unidades de TI, a las áreas de negocio o ser externalizado, lo que se busca es generar una sinergia en el diseño del marco de gobierno y gestión de TI y evitar de esta forma forzar la creación de estructuras o procesos dentro de la unidad de TI que no corresponden a esta, ya que, en muchos casos, las entidades y empresas supervisadas diseñan procesos a nivel de negocio que podrían incorporar las prácticas del marco de gobierno y gestión de TI.	
	[56]BAC De acuerdo a lo indicado en la sesión del 26 de abril 2024 con los reguladores, se solicita incluir en el reglamento la aclaración comentada en la sesión, con respecto a que los procesos indicados en el Anexo 1 Procesos de evaluación del marco de Gobierno y Gestión de TI, están basados en un marco de referencia y que como tal, la entidad puede implementarlos y evaluarlos de	**[56]Procede** Efectivamente, en el artículo 43 se establece que la entidad debe incluir en el perfil de TI los procesos de evaluación que le son aplicables.	

	acuerdo a su definición y apetito de riesgo, sin que esto signifique necesariamente que está obligada a implementar y evaluar todas las actividades que están incluidas en el marco de referencia. En este caso COBIT 2019.		
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.	**[57]QUÁLITAS** Que nos indiquen cuales estándares internaciones cumplen con las disposiciones establecidas en este reglamento.	**[57]No procede** El marco de regulación establece la expectativa del regulador, mientras que en aspectos de implementación queda a criterio de la entidad el cómo ejecutarlo. En consecuencia, la entidad es la que debe realizar el análisis para determinar si un estándar le permite cumplir con las disposiciones reglamentarias.	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.			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			**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:	**[58]BPDC** Se sugiere incluir "Asegurar el cumplimiento normativo y de la legislación nacional aplicable"	**[58]No procede** Ya está incluido en el inciso r).	El marco de gobierno y gestión de TI debe permitir a las entidades y empresas supervisadas cumplir con los siguientes propósitos:
	[59]COOPEALIANZA De la misma forma que se indicó en el punto anterior, al intentar cumplir con estos propósitos y tener el auditor que cumplir con la matriz de evaluación en su totalidad, no se permite a la entidad diseñar la metodología de acuerdo con su estrategia organizacional, el apetito de riesgo, el nivel de tolerancia al riesgo y las políticas aprobadas por el Órgano de Dirección.	**[59]Procede** Se ajustó la redacción de los artículos 43 y 46 para mejorar el entendimiento. En el anexo 1 “Procesos de evaluación del marco de gobierno y gestión de TI” se agregó lo siguiente a fin de atender lo indicado en la observación: “Los procesos de evaluación del marco de gobierno y gestión de TI están basados en marcos de referencia internacionales, por lo que, la evaluación de dichos	

		procesos se realizará 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. Por otra parte, en la Sección XII. Lineamientos relacionados con las auditorías externas de TI, ubicada en los lineamientos generales de la propuesta de modificación reglamentaria, se indica que, Las "prácticas de gobierno y gestión" establecidas en la matriz de evaluación serán adoptadas y adaptadas por las entidades y empresas supervisadas de conformidad con sus riesgos identificados.	
a) Orientar hacia la definición del gobierno de TI con un enfoque integrado y alineado con el gobierno corporativo.			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.	**[60]ISACA** b) recursos y servicios de TI	**[60]Procede** Se ajusta la redacción.	b) Asegurar un equilibrio entre el uso de los recursos de TI, servicios 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.			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.			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.	**[61]ISM** e) Asegurar que se identifica e involucra a las partes interesadas en el diseño del Sistema de gobierno y gestión de TI.	**[61] No procede** Se prefiere el término de "marco de gobierno y gestión de TI", el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y	e) Asegurar que se identifica e involucra a las partes interesadas en el diseño del marco de gobierno y gestión de TI.

		las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	
f) Diseñar e implementar el marco de gobierno y gestión de TI de conformidad con los objetivos y riesgos del negocio.	**[62]ISM** f) Diseñar e implementar el Sistema de gobierno y gestión de TI de conformidad con los objetivos y riesgos del negocio.	**[62] No procede** Se prefiere el término de "marco de gobierno y gestión de TI", el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	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.			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.			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.			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.			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.			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.			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.			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.			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.			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.	**[63]BNCR** Se recomienda incluir de manera específica el tema de seguridad de la información y la ciberseguridad. Es muy importante tenerlo presente en el entorno actual de amenazas cibernéticas que están en constante evolución. En el inciso p) se recomienda ampliar el inciso de la siguiente manera: "Asegurar la configuración y seguridad de los activos de información tecnológicos y la información que soportan, considerando la gestión, aceptación y transición de los cambios"	**[63]Procede** Se ajusta la redacción considerando parte de lo sugerido.	p) Asegurar la configuración y la seguridad de los activos de información, así como asegurar la información que dichos activos soportan, de conformidad con la gestión, aceptación y transición de los cambios.
	[64]ABC Sobre esta norma, resulta conveniente incluir el tema de la seguridad de la información y de la ciberseguridad. En lo que concierne al inciso p), se recomienda ampliar el inciso de la siguiente manera: "Asegurar la configuración y seguridad de los activos de información tecnológicos y la información que soportan, considerando la gestión, aceptación y transición de los cambios".	**[64]Procede** Se ajusta la redacción considerando parte de lo sugerido.	
	[65]CB Se recomienda incluir de manera específica el tema de seguridad de la información y la ciberseguridad. Es muy importante tenerlo presente en el entorno actual de amenazas cibernéticas que están en constante evolución. En el inciso p) se recomienda ampliar el inciso de la siguiente manera: "Asegurar la configuración y seguridad de los activos de información tecnológicos y la	**[65]Procede** Se ajusta la redacción considerando parte de lo sugerido.	

	información que soportan, considerando 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.			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.	**[66]COOPEFYL** ¿Con relación al propósito r) a las cooperativas de la regulación proporcional Acuerdo Sugef 25-23 se les exime de estos propósitos?	**[66]No procede (comentario)** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de	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.

		riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.			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			**Sección II. Responsabilidades del Órgano de Dirección**
Artículo 8. Responsabilidades generales sobre el gobierno de TI			**Artículo 8. Responsabilidades generales sobre el gobierno de TI**
En relación con el gobierno de TI, el Órgano de Dirección, al menos, debe:	**[67]BPDC** Se sugiere incluir: "Asegurar que exista una clara separación de la gobernanza y la gestión de Seguridad de la Información para prevenir los conflictos de intereses en la toma de decisiones."	**[67] No procede** En línea con lo sugerido por la entidad, se espera que exista un involucramiento de todas las instancias de la entidad con relación a los temas de TI.	En relación con el gobierno de TI, el Órgano de Dirección, al menos, debe:
	[68]BNCR 1-Se recomienda incluir un inciso que haga referencia a la gestión por parte del Órgano de Dirección, donde se conozca el rendimiento del marco de gobierno y los principales indicadores del proceso que supervisa. 2-Por otra parte, es necesario que se revisen con detalle las responsabilidades establecidas en las secciones II, III y IV, debido a que hay temas administrativos y operativos y se están asignando, sin considerar el principio de proporcionalidad. Por ejemplo, la Junta Directiva posee un rol de supervisión y la responsabilidad puede ir orientada en supervisar que la Alta Gerencia rinda cuentas respecto a cualquier desviación de la estrategia.	**[68]No procede** 1-El Reglamento de Gobierno Corporativo define que, el Órgano de Dirección debe establecer los mecanismos para llevar a cabo evaluaciones anuales sobre su gestión, la de sus comités y de sus miembros; así como las acciones a tomar en caso de que existan reservas o dudas sobre el desempeño de alguno de sus miembros. 2-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	

	[69]CB 1-Se recomienda incluir un inciso que haga referencia a la gestión por parte del Órgano de Dirección, donde se conozca el rendimiento del marco de gobierno y los principales indicadores del proceso que supervisa. 2-Por otra parte, resulta necesario que se revisen con detalle las responsabilidades establecidas en las secciones II, III y IV, debido a que hay temas administrativos y operativos y se están asignando, sin considerar el principio de proporcionalidad. Por ejemplo, la Junta Directiva posee un rol de supervisión y la responsabilidad puede ir orientada en supervisar que la Alta Gerencia rinda cuentas respecto a cualquier desviación de la estrategia.	**[69]No procede** 1-El Reglamento de Gobierno Corporativo establece que, el Órgano de Dirección debe establecer los mecanismos para llevar a cabo evaluaciones anuales sobre su gestión, la de sus comités y de sus miembros; así como las acciones a tomar en caso de que existan reservas o dudas sobre el desempeño de alguno de sus miembros. 2-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	
	[70]ISM Sistema en lugar de Marco	**[70] No procede** Se prefiere el término de “marco de gobierno y gestión de TI”, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término “marco” está más alineado con los fines regulatorios, mientras que el término sistema se	

		relaciona más con la implementación.	
	[71]ISACA ... Con relación al gobierno de TI ...	**[71] No procede** Le redacción es clara. Según la Real Academia Española lo adecuado es utilizar. “En relación con”.	
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.	**[72]COOPEFYL** Con relación al punto a): En el artículo No. 3 de este reglamento en consulta indican:" 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". ¿Como atienden las cooperativas que están exentas de este capítulo la presente aprobación del informe a remitir a la SUGEF, ya que el Acuerdo SUGEF 25-23 exime a las cooperativas de la administración de riesgo y en el anexo2 de los lineamientos incluye el proceso de gestión de riesgos? hay contradicción y además aumentan el ISP al 16%?	**[72]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se	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.

		incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se encuentra a disposición de las entidades. Por otra parte, el proyecto del Acuerdo SUGEF 25-23 tiene un marco considerativo que desarrolló todo el enfoque de proporcionalidad. Además, hay varias notas de respuesta dirigidas a Coopefyl mediante las cuales se le explica el enfoque de proporcionalidad, donde se expusieron los argumentos de la Superintendencia. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
b) Establecer un Comité de TI o una función equivalente y aprobar sus normas de gobierno y gestión.	**[73]POPULARPENSIONES** En relación al inciso b), para el caso de los Comités de TI conglomerales, el Órgano de Dirección no tiene las facultades para establecer el comité de TI, ni su normativa. Esta función recae en el órgano de Dirección del Conglomerado, por lo cual se propone que en los Comités Conglomerales, la función del Órgano de Dirección sea el nombramiento de sus representantes en dicho Comité de TI.	**[73]No procede** En el artículo 12, se establece que, 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.	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.			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.			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.			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.			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.			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			**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:	**[74]COOPEFYL** Las cooperativas del acuerdo 25-23 según la presente consulta estos temas no les aplica.? ¿Ni lo que está en los lineamientos asociado a estos temas?	**[74]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización	En relación con el gobierno de la seguridad de la información y de la seguridad cibernética, el Órgano de Dirección, al menos, debe:

		de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
	[75]BNCR 1-Se recomienda incluir un inciso que haga referencia a la gestión por parte del Órgano de Dirección, donde se conozca el rendimiento del marco de gobierno y los principales indicadores del proceso que supervisa. 2-Por otra parte, es necesario que se revisen con detalle las responsabilidades establecidas en las secciones II, III y IV, debido a que hay temas administrativos y operativos y se están asignando, sin considerar el principio de proporcionalidad. Por ejemplo, la Junta Directiva posee un rol de supervisión y la responsabilidad puede ir orientada en supervisar que la Alta Gerencia rinda cuentas respecto a cualquier desviación de la estrategia.	**[75]No procede** 1-El Reglamento de Gobierno Corporativo establece que El Órgano de Dirección debe establecer los mecanismos para llevar a cabo evaluaciones anuales sobre su gestión, la de sus comités y de sus miembros; así como las acciones a tomar en caso de que existan reservas o dudas sobre el desempeño de alguno de sus miembros. 2-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	
	[76]OPCCCSS Se entiende que estos 2 términos los quieren hacer uno solo. Pero actualmente existe responsabilidades y recursos de la seguridad que no tiene	**[76] No procede** La propuesta reglamentaria contiene las expectativas de alto nivel que las superintendencias esperan que las entidades y	

	acceso los encargados de Seguridad de la Información. Por lo que se tiene que tener claro que su cumplimento es una responsabilidad compartida con el Área de TI principalmente.	empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Por lo que, para las Superintendencias es relevante destacar el tema de la seguridad cibernética.	
	[77]CB 1-Se recomienda incluir un inciso que haga referencia a la gestión por parte del Órgano de Dirección, donde se conozca el rendimiento del marco de gobierno y los principales indicadores del proceso que supervisa. 2-Por otra parte, resulta necesario que se revisen con detalle las responsabilidades establecidas en las secciones II, III y IV, debido a que hay temas administrativos y operativos y se están asignando, sin considerar el principio de proporcionalidad. Por ejemplo, la Junta Directiva posee un rol de supervisión y la responsabilidad puede ir orientada en supervisar que la Alta Gerencia rinda cuentas respecto a cualquier desviación de la estrategia.	**[77]No procede** 1-El Reglamento de Gobierno Corporativo establece que, el Órgano de Dirección debe establecer los mecanismos para llevar a cabo evaluaciones anuales sobre su gestión, la de sus comités y de sus miembros; así como las acciones a tomar en caso de que existan reservas o dudas sobre el desempeño de alguno de sus miembros. 2-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	
	[78]ISACA ... Con relación al gobierno de la seguridad ...	**[78] No procede** Le redacción es clara. Según la Real Academia Española lo adecuado es utilizar. “En relación con”.	
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.	**[79]BPDC** Para el punto (a) se debe confirmar si el Sistema de Gestión de Seguridad de la Información debe ser certificado o no.	**[79]No procede** En ningún caso el marco de regulación hace referencia que la entidad deba certificarse o deba certificar algún proceso de TI. La disposición no hace referencia a “sistema de seguridad de la información”.	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.			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.			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.			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			**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:	**[80]BNCR** 1-Se recomienda incluir un inciso que haga referencia a la gestión por parte del Órgano de Dirección, donde se conozca el rendimiento del marco de gobierno y los principales indicadores del proceso que supervisa. 2-Por otra parte, es necesario que se revisen con detalle las responsabilidades establecidas en las secciones II, III y IV, debido a que hay temas administrativos y operativos y se están asignando, sin considerar el principio de proporcionalidad. Por ejemplo, la Junta Directiva posee un rol de supervisión y la responsabilidad puede ir orientada en supervisar que la Alta Gerencia rinda cuentas respecto a cualquier desviación de la estrategia.	**[80]No procede** 1-El Reglamento de Gobierno Corporativo establece que, el Órgano de Dirección debe establecer los mecanismos para llevar a cabo evaluaciones anuales sobre su gestión, la de sus comités y de sus miembros; así como las acciones a tomar en caso de que existan reservas o dudas sobre el desempeño de alguno de sus miembros. 2-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	En relación con el gobierno de la resiliencia operativa digital, el Órgano de Dirección, al menos, debe:
	[81]CB 1-Se recomienda incluir un inciso que haga referencia a la gestión por parte del Órgano de Dirección, donde se conozca el rendimiento del marco de gobierno y los principales indicadores del proceso que supervisa. 2-Por otra parte, resulta necesario que se revisen con detalle las responsabilidades establecidas en las secciones II, III y IV, debido a que hay temas administrativos y operativos y	**[81]No procede** 1-El Reglamento de Gobierno Corporativo establece que, el Órgano de Dirección debe establecer los mecanismos para llevar a cabo evaluaciones anuales sobre su gestión, la de sus comités y de sus miembros; así como las acciones a tomar en caso de que existan reservas o dudas sobre el desempeño de alguno de sus miembros.	

	se están asignando, sin considerar el principio de proporcionalidad. Por ejemplo, la Junta Directiva posee un rol de supervisión y la responsabilidad puede ir orientada en supervisar que la Alta Gerencia rinda cuentas respecto a cualquier desviación de la estrategia.	2-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	
	[82]ISACA Con relación al gobierno ...	**[82] No procede** Le redacción es clara. Según la Real Academia Española lo adecuado es utilizar: “En relación con”.	
a) Aprobar las políticas de resiliencia operativa digital de la entidad o empresa supervisada.			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.			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.			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.			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.			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			**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			**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:	**[83]ISM** Sistema en lugar de Marco	**[83] No procede** Se prefiere el término de “marco de gobierno y gestión de TI”, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y	En relación con el gobierno y la gestión de TI, la Alta Gerencia, al menos, debe:

		las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	
	[84]ISACA Con relación al gobierno ...	**[84] No procede** Según la Real Academia Española lo adecuado es utilizar: "En relación con".	
a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección.			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.	**[85]COOPEFYL** ¿Esto no le aplica a las cooperativas del Acuerdo SUGEF 25-23? ¿Con relación al punto d) las cooperativas dentro del acuerdo SUGEF 25-23 se les exime de estas responsabilidades?	**[85]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión	b) Proponer al Órgano de Dirección la estrategia y los recursos requeridos para la implementación del marco de gobierno y gestión de TI.

		de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se encuentra a disposición de las entidades. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
	[86]ABC La formulación y aprobación de estrategias por la Alta Gerencia y la asignación de recursos puede generar una carga administrativa importante.	**[86]No Procede** Esta disposición se alinea con los aspectos normados en el Acuerdo CONASSIF 4-16.	
c) Implementar las políticas relacionadas con TI aprobadas por el Órgano de Dirección.			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.			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.			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.	**[87]POPULARPENSIONES** En relación al inciso f), establecer medidas es una tarea de bajo nivel que requiere de un conocimiento técnico específico, se propone cambiar el verbo por Aprobar o apoyar la implementación.	**[87]Procede** Se ajusta la redacción considerando parte de lo indicado en la observación.	f) Asegurar que se establezcan~~er~~ 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.			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.			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			**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.	**[88]COOPEFYL** Con esta normativa en consulta Coopefyl R.L. no está obligada con tener este Comité, según indica el artículo 3 de este reglamento ya que lo dispuesto en los capítulos II y III que se indican a continuación se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades y ¿ Si se asumen nos ajustarían el porcentaje de SP? , porque por un lado indican que nos suben el indicador de SP pero por otro lado hay que gestionar el gobierno corporativo y la gestión de riesgos. ¿Las cooperativas dentro del Acuerdo Sugef 25-23, se les exime de estas responsabilidades?	**[88]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información;	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.

		se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. El proyecto del Acuerdo SUGEF 25-23 no está siendo sujeto de ajuste en esta oportunidad; dicho proyecto tuvo su matriz de observaciones en la cual se incluyeron las explicaciones a los comentarios de las entidades, entre estas, Coopefyl. Dicha matriz se encuentra a disposición de las entidades. Por otra parte, el proyecto del Acuerdo SUGEF 25-23 tiene un marco considerativo que desarrolló todo el enfoque de proporcionalidad. Además, hay varias notas de respuesta dirigidas a Coopefyl mediante las cuales se le explica el enfoque de proporcionalidad, donde se expusieron los argumentos de la Superintendencia. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
	[89]ISM Sistema en lugar de Marco	**[89] No procede** Se prefiere el término de “marco de gobierno y gestión de TI”, el	

		cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	
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.			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.			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	**[90]BNVITAL** Sobre el párrafo "n 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	**[90]No procede** No es necesario, dado que, todo acto administrativo como el señalado en la observación requiere un análisis sustentado.	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.	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." El párrafo requiere precisión, Por lo que se recomienda valorar redacción a "En el caso de que la Superintendencia, mediante la aplicación de un estudio sobre este órgano determine que ..."		un Comité individual de TI para la respectiva entidad o empresa.
Artículo 13. Responsabilidades del Comité de TI o de la función equivalente			**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:	**[91]BCR** Sobre el artículo 13 por favor clarificar o detallar ¿cómo se incorpora la función de la gestión de riesgos, requerida para el abordaje integral de implementación y mantenibilidad de este reglamento en la organización y desde el Comité de TI o su función equivalente? – no queda claro el rol y responsabilidades de este comité respecto al abordaje y cumplimiento de una adecuada gestión de riesgos. Conforme con el Acuerdo Conassif 4-16, el órgano de dirección tiene la potestad de crear los comités de apoyo, en este sentido recomendamos incluir como parte de las funciones del CCTI, funciones que apoyen las nuevas funciones (Ciberseguridad, Seguridad de información, Resiliencia operativa Digital) que se le asigna al órgano de dirección.	**[91]No procede** Conviene aclarar sobre la actualización que sufrido el marco de regulación en el tiempo; el aspecto señalado por la entidad ha sido superado con la emisión del Acuerdo SUGEF 2-10 que delimitó con mayor claridad estos temas. Lo señalado por la entidad se disponía en el Reglamento sobre la gestión de la tecnología de información, Acuerdo Sugef 14-09, ya derogado.	Corresponden al Comité de TI o a la función equivalente, al menos, las siguientes responsabilidades:
	[92]CB Se solicita clarificar o detallar ¿cómo se incorpora la función de la gestión de riesgos, requerida para el abordaje integral de implementación y	**[92]No procede** Conviene aclarar sobre la actualización que sufrido el marco de regulación en el tiempo; el aspecto señalado por la entidad ha	

	mantenibilidad de este reglamento en la organización y desde el Comité de TI o su función equivalente? – no queda claro el rol y responsabilidades de este comité respecto al abordaje y cumplimiento de una adecuada gestión de riesgos.	sido superado con la emisión del Acuerdo SUGEF 2-10 que delimitó con mayor claridad estos temas. Lo señalado por la entidad se disponía en el Reglamento sobre la gestión de la tecnología de información, Acuerdo Sugef 14-09, ya derogado.	
	[93]BAC El artículo 13 sobre Responsabilidades del Comité de TI o de la función equivalente, se declaran funciones que el Comité de TI establecido debe de cumplir, sin embargo, en el Lineamiento en la Sección I. Lineamientos relacionados con el reconocimiento de la gestión de TI, del Comité de TI o sus funciones equivalentes como corporativos, se declaran las funciones del Comité de TI que estén tipificados como Corporativos. ¿Con cuál de los dos grupos de funciones definidos, es que se deben de cumplir cuando ya se trabaja con carácter Corporativo?	**[93]No procede** En lo lineamientos lo que se indican son las condiciones que las entidades y empresas supervisadas considerarán para tipificar su gestión de TI, Comité de TI o funciones equivalentes como corporativos. En este artículo 13 lo que se establecen son las responsabilidades del Comité de TI.	
a) Supervisar la implementación del marco de gobierno y gestión de TI.	**[94]ISM** 1-Supervisar la implementación del Sistema de gobierno y gestión de TI. 2-Estas responsabilidades están restringiendo la capacidad del comité a un ente que filtra y valida simplemente. El avance que varias organizaciones han tenido con respecto a la delegación del Órgano de Dirección al Comité, para que sea una estructura realmente de soporte al gobierno, capaz de tomar cierto nivel de decisión, retrocedería. Como mínimo debería dejarse una responsabilidad general que permita a	**[94]No procede** El término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación. 2- El balance que se desea dar es que el Órgano de Dirección puede apoyarse en este tipo de Comités. El artículo 6 del Reglamento de Gobierno Corporativo establece que el Órgano de Dirección es responsable de aprobar la estructura organizacional y funcional de la entidad y que eso	a) Supervisar la implementación del marco de gobierno y gestión de TI.

	estas empresas continuar su dinámica y avanzar en la agilidad operativa.	implica, entre otros aspectos lo siguiente: “Constituir y establecer la conformación de los comités técnicos, unidades y cualquier otra instancia que el Órgano de Dirección considere pertinente para la buena gestión de la entidad y de los Vehículos de Administración de Recursos de Terceros; para ello, los dota de los recursos, independencia, autoridad y jerarquía necesarios para su operación. Aunado a lo anterior, en el artículo 1. Objeto, de la presente modificación reglamentaria, se indica que: “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.	
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.	**[95]ISACA** b) ... metas de TI. Asimismo, ...	**[95]No procede** La redacción incorporada en el considerando es clara.	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.	**[96]ISM** c) Cumplir con las funciones o responsabilidades de soporte al gobierno, que le sean delegadas por el Órgano de Dirección.	**[96]No procede** Lo indicado en la observación es algo inherente a las responsabilidades del Comité de conformidad con lo establecido en el Reglamento de Gobierno Corporativo.	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.	**[97]ISACA** d) ... cuando corresponda, atender las observaciones ...	**[97]No procede** La redacción incorporada en el considerando es clara.	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.			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.			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.	**[98]BNVITAL** Sobre el inciso g). La validación de los conocimientos y la experiencia para auditar aspectos de seguridad de información, así como, el resto de los temas de este tipo de auditorías se realiza como parte de la redacción del pliego cartelario y basado en los requerimientos solicitados por Supervisor y los derivados del análisis interno de la empresa. Por lo que no se considera adecuada esta función para el Comité de TI.	**[98]No procede** Tal como lo indica la observación, la validación de los conocimientos y la experiencia para auditar aspectos de seguridad de información, así como, el resto de los temas de este tipo de auditorías se podría realizar como parte de la redacción del pliego cartelario, sin embargo, la propuesta reglamentaria contiene las expectativas que las Superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio.	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 u otros aspectos, de conformidad con el alcance solicitado.
	[99]ISACA g) ... o el auditor externo de TI independiente, cuenten con los conocimientos ...	**[99] No procede** Se guarda la congruencia con la terminología utilizada en el Reglamento General de Auditores Externos, Acuerdo Conassif 1-10.	
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.			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			**Sección IV. Responsabilidades de los Órganos de Control**
Artículo 14. Responsabilidades sobre la Auditoría Interna o de la función equivalente			**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:	**[100]QUÁLITAS** Se tendría que disponer de un nuevo recurso o capacitación con formación en T.I, para abarcar estos temas, implicaría un costo adicional para las empresas. El auditor interno tiene	**[100]No procede** Como parte de la supervisión del gobierno corporativo, las Superintendencias poder requerir trabajos específicos sobre aspectos de interés del supervisor.	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:

	compromiso de reportar inconsistencias al ente supervisado, pero no trabajos para ellos por eso se presenta a la Junta Directiva el plan anual de trabajo.	Este requerimiento es consistente con lo que se dispone en el Reglamento de Gobierno Corporativo. Además, estos requerimientos pueden estar dirigidos al Órgano de Dirección quien lo incorpora al plan de trabajo de la Auditoría Interna. La integración de las tecnologías de la información en los modelos de negocio, junto con su creciente dependencia, plantea la aparición de nuevos riesgos que, de materializarse, podrían exponer a las entidades y empresas supervisadas. En este contexto, se espera que la entidad cuente con la capacidad de evaluar la gestión de riesgos relacionados con las tecnologías de la información como parte de su tercera línea de defensa.	
	[101]COOPEFYL Esto no aplica para las cooperativas de regulación proporcional según el artículo 3 del presente reglamento.	**[101]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica	

		que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
a) Revisar y asegurar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.	**[102]BPDC** Inciso a). No es función de la auditoría asegurar el cumplimiento, pero si verificar/validar el cumplimiento, caso contrario identificar el incumplimiento y solicitar acciones correctivas	**[102]Procede** Se ajusta la redacción.	a) ~~Revisar y asegurar~~ Verificar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.
	[103]ISACA a) ... que se establezcan con relación a TI	**[103] No procede** Según la Real Academia Española lo adecuado es utilizar: “En relación con”.	
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.	**[104]ISM** b) Implementar un plan de auditoría basado en el riesgo para evaluar la calidad y la eficacia del Sistema de gobierno y gestión de TI, de la seguridad de la información y de la seguridad cibernética.	**[104]No procede** Se prefiere el término de “marco de gobierno y gestión de TI”, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de	b) Implementar un plan de auditoría basado en el riesgo, el cual, permita ~~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.

		una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	
	[105]ISACA b) basado en el riesgo que permita evaluar la calidad ...	**[105]Procede** Se ajusta la redacción.	
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.	**[106]BCR** ¿Cuál es el alcance esperado de la evaluación de la calidad y eficiencia de los planes de acción? ¿A cuál órgano se debe rendir el resultado de la evaluación?, ¿Cuál es la periodicidad en la que se debe efectuar dicha evaluación? ¿En qué momento se debe llevar a cabo dicha evaluación?	**[106]No procede** Lo referente a planes de acción para entidades supervisadas por SUGEF está regulado en el artículo 22. "Planes de acción y saneamiento eficaces" del Acuerdo SUGEF 24-22.	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.			d) Ejecutar trabajos específicos requeridos por las Superintendencias.
Artículo 15. Responsabilidades de la unidad o función de gestión de riesgos			**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:	**[107]QUÁLITAS** Se tendría que disponer de un nuevo recurso con formación en T.I, para abarcar estos temas, implicaría un costo adicional para la empresa.	**[107]No procede** Esta es la expectativa del regulador. Para el cierre de las brechas que pueda tener la entidad en relación con las disposiciones del presente reglamento, se incluyó un transitorio séptimo.	En relación con las tecnologías de información, la unidad o función de gestión de riesgos, al menos, debe:
	[108]COOPEFYL Esto no aplica para las cooperativas de regulación proporcional según el artículo 3 del presente reglamento en	**[108]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones	

	consulta.? Tampoco los temas desarrollados en los lineamientos generales relacionados con estos puntos.?	sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.	**[109]BPDC** En el punto a, debe quedar claro que esto se desarrollará sobre los procesos definidos en el Plan de Trabajo de la Auditoría Interna para cada año, incluso sería solo para el alcance	**[109]No procede** Lo sugerido es un aspecto de índole operativa. Por otra parte, no se identifica una relación clara entre lo sugerido en la observación	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.

	definido en la planificación del estudio, porque incluso en la evaluación de los procesos no necesariamente se abarca todo, a pesar de que sí tenemos definido como base de nuestro Universo Auditable el marco de trabajo Cobit.	y el contenido de lo dispuesto en el inciso a).	
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.	**[110]ISACA** Con relación a las tecnologías ... b) Considerar la declaración del apetito, tolerancia y capacidad de los riesgos de la entidad o empresa supervisada, para gestionar los riesgos tecnológicos, de tecnologías emergentes, de seguridad de la información y de seguridad cibernética	**[110] No procede** El enfoque dado aquí es congruente con el marco de regulación vigente en materia de riesgos y gobierno corporativo.	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.			c) Ejecutar trabajos específicos requeridos por las Superintendencias.
CAPÍTULO III			**CAPÍTULO III**
ORGANIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN			**ORGANIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN**
Sección I. Generalidades de la gestión de TI			**Sección I. Generalidades de la gestión de TI**
Artículo 16. Gestión de TI individual o función corporativa			**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.	**[111]COOPEFYL** No aplica para las cooperativas de regulación proporcional según el artículo 3 del presente reglamento en consulta pública. Tampoco le aplica los lineamientos generales asociados a estos temas? Los plazos son naturales o hábiles, así como las horas en el reglamento, ya que la SUGEF no trabaja 24/7 ni en días feriados.	**[111]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas.	La gestión de TI de las entidades y empresas supervisadas es tipificada de manera predeterminada como gestión de TI individual.

		De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos. Por otra parte, en la disposición no se definen plazos.	
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.			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			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.			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.	**[112]BNVITAL** Sobre el párrafo "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 párrafo requiere precisión, Por lo que se recomienda valorar redacción a "En el caso de que la Superintendencia, mediante la aplicación de un estudio sobre este órgano determine que ..."	**[112]No procede** No es necesario, dado que, todo acto administrativo como el señalado en la observación requiere un análisis sustentado.	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.			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			**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.	**[113]BPDC** ¿Qué pasa en conglomerados donde la función de TI está adscrita a la entidad más grande dando soporte a otras empresas del conglomerado?	**[113]No procede** Por una parte, la sección I de los lineamientos generales contiene las disposiciones que deben cumplirse para que las entidades reconozcan su gestión de TI como corporativa, dentro de las cuales, se indica: “Alguna de las entidades o empresas supervisadas preste los servicios de TI a otras entidades o empresas de su mismo grupo o conglomerado financiero”.	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.

		Por otra parte, las entidades y empresas supervisadas que formen parte de un grupo o conglomerado financiero deberán de suscribir los respectivos contratos y acuerdos de niveles de servicio, para mitigar los riesgos que existan con relación a terceros incluyendo su casa matriz, tal como lo indica el reglamento.	
	[114]COOPEALIANZA Se solicita la siguiente redacción: 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 contribuir con la implementación del marco de gobierno y gestión empresarial de la entidad. Lo anterior para reforzar el aspecto de que este es un marco de gobierno y gestión empresarial donde interviene toda la organización y no sólo TI.	**[114] No procede** El reglamento utiliza una terminología que está con consonancia con el resto de la normativa aprobada por el CONASSIF. En virtud de lo anterior, el término "empresarial", no se utiliza, ya que, en el contexto de la regulación se usa como sinónimos los términos organización, así como entidades o empresas supervisadas. Cabe destacar que como parte del Marco de Gobierno y Gestión de TI existen procesos de TI que pueden ser diseñados e implementados de forma transversal en las organizaciones y no específicamente en las áreas de TI, tales como riesgos, auditoria, control, seguridad de la información, recursos humanos, gestión de calidad, gestión de proveedores, entre otros.	
Artículo 18. Responsabilidades de la unidad de TI o de la función equivalente			**Artículo 18. Responsabilidades de la unidad de TI o de la función equivalente**
La Unidad de TI o la función equivalente es responsable de:			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.	**[115]ISM**	**[115]No procede**	a) Ejecutar las estrategias para la implementación del marco de gobierno y gestión de TI.

	a) Ejecutar las estrategias para la implementación del Sistema de gobierno y gestión de TI.	Se prefiere el término de “marco de gobierno y gestión de TI”, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico y operativo de la tecnología de la información. Por lo tanto, el término “marco” está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	
b) Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos establecidos.			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.	**[116]BCR** Se recomienda ajustar la redacción del inciso c) de la siguiente forma: “Diseñar e implementar la arquitectura tecnológica, la arquitectura de información y de aplicaciones alineada a la arquitectura de negocio, a fin de soportar las operaciones de la entidad o empresa supervisada.”	**[116]Procede** Se ajusta la redacción.	c) Diseñar e implementar la arquitectura tecnológica ~~y de aplicaciones alineada a,~~ la arquitectura de información y de aplicaciones, alineadas a la arquitectura de negocio ~~y a la arquitectura de información~~, a fin de soportar las operaciones de la entidad o empresa supervisada.
	[117]ISACA c) No se ha establecido con anterioridad que la organización debe establecer las arquitecturas de negocio y de información, por lo que podría	**[117]No procede** En el artículo 7. Propósitos del marco de gobierno, el inciso h), indica que, unos de los propósitos del citado marco es establecer una dirección y una estructura	

	limitar el diseño de la arquitectura tecnológica	eficiente para gestionar TI; además, alinear los objetivos de la entidad o empresa supervisada con el uso de la tecnología y su arquitectura organizacional.	
	[118]OPCCCSS En el punto c) del artículo 18 de Reglamento se indica que una de las responsabilidades de la Unidad de TI o de la función equivalente es "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", sin embargo, si como parte del estudio técnico para determinar los procesos que aplican a la entidad, se determina que el proceso de gestionar la arquitectura empresarial no se debe implementar, esta función no se podría aplicar. Por lo tanto, se sugiere revisar dicha función.	**[118]No procede** La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Por lo que, se espera que las entidades establezcan los controles mínimos para gestionar su arquitectura organizacional.	
	[119]CB Inciso c): Se sugiere ajustar la redacción del inciso c) de la siguiente forma: "Diseñar e implementar la arquitectura tecnológica, la arquitectura de información y de aplicaciones alineada a la arquitectura de negocio, a fin de soportar las operaciones de la entidad o empresa supervisada."	**[119]Procede** Se ajusta la redacción.	
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.			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.	**[120]BAC** Se solicita considerar una modificación al texto del punto 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, por, e) Asegurar que los bienes y servicios de TI críticos estén identificados, además, asegurar que se mantengan disponibles y que sean gestionados de acuerdo a la necesidad de negocio. (Artículo 18. Responsabilidades de la unidad de TI o de la función equivalente)	**[120]No procede** La redacción sugerida en la observación podría generar confusión.	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.	**[121]BNCR** En el inciso f se sugiere modificar el párrafo de la siguiente manera: "Diseñar un modelo de arquitectura para soportar las operaciones de la entidad o empresa supervisada y garantizar su continuidad ante eventos disruptivos".	**[121]No procede** Lo sugerido en la observación está relacionado con el inciso c), cuya redacción es clara.	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			**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			**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.	**[122]BCR** Incluir en el Artículo 4, los conceptos de activos de información primarios y activos de información de apoyo.	**[122]No procede** Los conceptos indicados ya están contemplados en la "Sección II. Lineamientos relacionados con el modelo de clasificación de los activos de información", contenida en los lineamientos generales de la propuesta de modificación regulatoria.	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.
	[123]CB Incluir en el apartado correspondiente, los conceptos de activos de	**[123]No procede** Los conceptos indicados ya están contemplados en la "Sección II.	

	información primarios y activos de información de apoyo.	Lineamientos relacionados con el modelo de clasificación de los activos de información", contenida en los lineamientos generales de la propuesta de modificación regulatoria.	
	[124]ISACA Considerar: - no mezclar la definición de activo digital con activo de información. - refrasear el uso de palabras como "adecuado", "eficiente", "efectivo" y que declaren concretamente qué deben cumplir las entidades para estar allí, poniendo un límite claro a la interpretación de cualquier persona, garantizando el cumplimiento, ante todo. - la definición de información crítica la deben ligar al proceso de identificación, clasificación y valoración de activos de información para que igualmente sea concreta su definición y alcance. - dónde se menciona la separación de registros por empresas del grupo, no me queda claro que esperan, ya que esto puede atentar contra la experiencia de un usuario de servicios financieros y productos diferentes ofrecidos por un mismo grupo, lo que haría que en lugar de poder verlo de forma integral cada empresa lo vea como si fuese un cliente diferente.	**[124]No procede** En la propuesta de artículo no se hace referencia a lo indicado en la observación.	
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.			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.			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			**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.	**[125]BPDC** Se indica que la superintendencia tendrá acceso irrestricto a bases de datos, sistemas y soluciones tecnológicas para sus labores de supervisión. Sin embargo, acceso sin ningún tipo de restricción o condición puede poner en riesgo la integridad de la información por manipulación indebida por parte de la superintendencia. Se entiende un acceso total de lectura y navegación, pero no debería poder modificar datos o cambiar configuraciones de forma intencionada o no intencionada.	**[125] No procede** Para efecto de un adecuado ejercicio de la práctica supervisora el acceso a información es fundamental, particularmente en situaciones de intervención de entidades. Las Superintendencias están sujetas a un estricto régimen de confidencialidad que asegura al sector supervisado la confianza de un adecuado manejo de los datos actuales y futuros. Cabe destacar que, en la práctica supervisora las Superintendencias, como parte de sus labores, no manipulan las bases de datos y, cuando corresponda, se requiere a las entidades o empresas supervisadas, la información dentro del ámbito de cada estudio realizado por los supervisores, salvaguardando en todo momento los principios de seguridad de la información (integridad y confidencialidad); sin dejar de lado el respeto, la protección y el tratamiento de los datos personales, de conformidad con la legislación vigente.	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.
	[126]QUÁLITAS No estamos de acuerdo ya que si debe haber restricciones y condiciones del porque quieren solicitar bases de datos ya que la empresa es responsable de la información resguardada.	**[126] No procede** Ver respuesta de la observación 125.	

	No es necesario el acceso ilimitado, debe ser al necesario para la supervisión (privacidad de datos). Aclarar que es acceso cuando lo pidan, no es un acceso abierto. Proveedores tienen acceso a DB´s que no tienen datos sensibles, no solo la empresa o el grupo. Aclarar como SUGESE hará el manejo de esas bases en caso de tener acceso, como resguardará SUGESE esos datos en caso potencial que lo pidan.		
	[127]VIDAPLENA Se considera que se debe mejorar la redacción de este articulo o realizar algún tipo de aclaración; porque hacer la indicación de que sin ningún tipo de restricción o condición, no es aplicable para un reglamento, cuando normalmente se mantiene en las bases de datos la información de terceros ya sean clientes o afiliados, y que se debe aplicar por ejemplo la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.	**[127]No procede** Ver respuesta de la observación 125.	
	[128]ABC Mantener acceso irrestricto por parte de las Superintendencias a todas las bases de datos, sistemas y aplicaciones compromete la seguridad de la información.	**[128]No procede** Ver respuesta de la observación 125.	
	[129]CB Según dispone este artículo, 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	**[129]No procede** La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Cabe destacar que, en la práctica supervisora las Superintendencias,	

	procesan o dan acceso a las bases de datos de las entidades. Debido a esto, ¿las instituciones deberán dar acceso a realizar las modificaciones en las bases de datos? Es claro que la función es de supervisión, pero si se da acceso libre al personal de la Superintendencia podría voluntaria o involuntariamente hacer modificaciones en los datos de la institución. Por lo tanto, la restricción debería ser de lectura total, pero sin derecho a escribir/sobrescribir. Asimismo, se solicita clarificar este alcance en caso de servicios tercerizados o en la nube.	como parte de sus labores, no manipulan las bases de datos y, cuando corresponda, se requiere a las entidades o empresas supervisadas, la información dentro del ámbito de cada estudio realizado por los supervisores, salvaguardando en todo momento los principios de seguridad de la información (integridad y confidencialidad); sin dejar de lado el respeto, la protección y el tratamiento de los datos personales, de conformidad con la legislación vigente.	
	[130]BAC Se puede aclarar qué se entiende por "separación de los registros de cada entidad", para el caso de que exista una base de datos compartidas entre las entidades del conglomerado	**[130]No procede** La separación de registros de cada entidad hace referencia a que la entidad o empresa supervisada debe garantizar en todo momento que se puede identificar el origen de las transacciones cuando existan plataformas compartidas por entre entidades y empresas que forman parte de un conglomerado o grupo financiero, asegurando en todo momento que 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.	
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			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.			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.	**[131]MUCAP** No existe claridad si dentro del perfil tecnológico se deben reportar todas las bases de datos incluyendo las de los ambientes de producción y también de pruebas o solo las de los sistemas críticos.	**[131] Procede** Por el nivel de detalle que requiere este aspecto, la información se encuentra en las guías para el llenado del perfil tecnológico.	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			**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.	**[132]ABC** La cantidad de obligaciones y medidas de control que se deben cumplir para la adquisición de software podría generar una barrera de entrada importante para proveedores tecnológicos más pequeños.	**[132] No procede** El aspecto esencial está dirigido a la debida diligencia que deben realizar las entidades en relación con proveedores. Las entidades y empresas supervisadas deben valorar los riesgos asociados al realizar contrataciones con proveedores que respondan a nuevos emprendimientos (Startups, Fintech entre otras) y PYMES tecnológicas. Las entidades y empresas supervisadas deben establecer los controles para garantizar que sus proveedores cumplan con los mismo requisitos y controles que tiene la entidad sobre sus bienes y servicios. En todo caso, la externalización de bienes y servicios no puede poner en riesgo la estabilidad de la entidad.	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.			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			**Sección III. Gestión de la computación en la nube**

Artículo 22. Servicios de 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.			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.	**[133]BNCR** Se sugiere modificar el segundo párrafo de la siguiente manera: "Cuando las entidades y empresas supervisadas deleguen sus procesos críticos a través de servicios de computación en la nube, deben establecer el modelo de responsabilidades compartidas para proteger la infraestructura en la que se ejecutan los servicios que se ofrecen en la nube y garantizar la seguridad de la información que se resguarde en estas infraestructuras.	**[133]No procede** El término de "modelo de responsabilidades compartidas" se puede prestar para confusión fuera el ámbito técnico, dado el involucramiento que se espera por parte de las instancias de gobierno corporativo. Dentro del contexto del reglamento el hecho de establecer las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube corresponde a lo que en la industria comúnmente se conoce como "modelo de responsabilidades compartidas".	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.
	[134]BCR Se solicita detallar cómo tratar los casos de información clasificada como sensible o crítica para la continuidad de negocio.	**[134]No procede** Son las entidades las que deben definir mediante sus políticas y procedimientos el tratamiento que darán a los casos de información clasificada como sensible o crítica para la continuidad de negocio.	
	[135]ABC En cuanto a las condiciones para brindar el servicio, debe considerarse que algunas marcas internacionales reconocidas ya establecen estas condiciones y no son negociables para las entidades locales, por lo que no es un aspecto sobre el cual se tenga control.	**[135]No procede** La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio, cuando se externalizan bienes y servicios	

		críticos de TI a través de proveedores de servicios en la nube. Es responsabilidad de la entidad realizar las valoraciones de riesgo cuando se delegue procesos a terceros y definir los mecanismos para establecer las responsabilidades. Cabe destacar que esta propuesta incorporar parte de las recomendaciones de los representantes de principales proveedores de servicios de computación en la nube. Adicionalmente, dentro del contexto del reglamento el hecho de establecer las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube corresponde a lo que en la industria comúnmente se conoce como "modelo de responsabilidades compartidas".	
	[136]CB En el artículo 22 de la sección III, capítulo III hace referencia al manejo de servicios de nube, sin embargo, se solicita acotar y tener en cuenta los contratos de adhesión, ya que no pueden ser modificados ante las grandes empresas que ofrecen servicio en la nube como por ejemplo AWS, Oracle, Microsoft, entre otras. Asimismo, se solicita detallar cómo tratar los casos de información clasificada como sensible o crítica para la continuidad de negocio.	**[136]No procede** El término de "modelo de responsabilidades compartidas" se puede prestar para confusión fuera el ámbito técnico, dado el involucramiento que se espera por parte de las instancias de gobierno corporativo. Dentro del contexto del reglamento el hecho de establecer las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube corresponde a lo que en la	

	Se sugiere modificar el párrafo segundo de la siguiente manera: "Cuando las entidades y empresas supervisadas deleguen sus procesos críticos a través de servicios de computación en la nube, deben establecer el modelo de responsabilidades compartidas para proteger la infraestructura en la que se ejecutan los servicios que se ofrecen en la nube y garantizar la seguridad de la información que se resguarde en estas infraestructuras.	industria comúnmente se conoce como "modelo de responsabilidades compartidas".	
Artículo 23. Obligaciones generales para el uso de la computación 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:	**[137]BNVITAL** No queda claro si es para los nuevos servicios o también debe aplicarse los vigentes.	**[137]No procede** La redacción indica: "Las entidades y empresas supervisadas que utilicen servicios de computación en la nube…". Por lo que, es para todos los casos en que se utilicen servicios de computación en la nube. Para el cierre de las brechas que pueda tener la entidad en relación con las disposiciones del presente reglamento, se incluyó un transitorio séptimo.	Las entidades y empresas supervisadas que utilicen servicios de computación en la nube deben:
	[138]BNCR 1-Se sugiere incluir otra obligación: "Asegurar la configuración del servicio en la nube que cumpla con los parámetros y políticas de seguridad definidas por la organización". 2-Con respecto al inciso l., se debe asegurar también que la empresa contratante del servicio tenga acceso a las llaves criptográficas de estos canales de comunicación.	**[138] No procede** 1-La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio, cuando se externalizan bienes y servicios críticos de TI a través de proveedores de servicios en la nube.	

		2- Son las entidades y empresas supervisadas las que deben establecer los controles técnicos de conformidad con su tamaño, complejidad, modelo de negocio y riesgos.	
a) Gestionar los riesgos derivados del uso de servicios de computación en la nube.			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.			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.	**[139]COOPEFYL** ¿Esto significa que no podemos tener proveedores que manejen información de clientes si no tiene al menos esa certificación? Esto a pesar de hacerles alguna evaluación de riesgos u otra revisión.	**[139]No procede** 1-La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio, cuando se externalizan bienes y servicios críticos de TI a través de proveedores de servicios en la nube. Se considera que la certificación ISO 27001 permite dar razonabilidad sobre la gestión de la seguridad de la información.	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.
	[140]OPCCCSS 1. No se aclara en el punto c cuáles estándares o mejores prácticas sustituyen o modifican la certificación ISO 27001, dado que se especifica que el proveedor debe contar obligatoriamente al menos con esa. Esto da entender que no se puede contar con proveedores que no posean al menos dicha certificación.	**[140]No procede** Se considera que la certificación ISO 27001 permite dar razonabilidad sobre la gestión de la seguridad de la información, por lo que, es un aspecto que las entidades deberán observar.	
	[141]PROMERICA En cuanto al punto c) Esto significa que no podemos tener proveedores que	**[141]No procede** Se considera que la certificación ISO 27001 permite dar	

	manejen información de clientes si no tiene al menos esa certificación? Esto a pesar de hacerles alguna evaluación de riesgos u otra revisión.	razonabilidad sobre la gestión de la seguridad de la información, por lo que, es un aspecto que las entidades deberán observar.	
	[142]BAC 1. Se considera que el punto C se delimitó y no da posibilidad de evaluar otras certificaciones que pueda poseer el proveedor a contratar. A su vez cerrar el requisito al cumplimiento de la ISO27001 puede ser restrictivo y no es garantía de un grado específico de Ciber Resiliencia. Deberían brindarse alternativas que generen confianza en la contratación. 2. Se entiende que las certificaciones son requeridas de acuerdo con la clasificación de los datos que se vayan a compartir con el proveedor. Por ejemplo, si se trata de información sensible. 3. ¿El supervisado puede aplicar su propia valoración para los servicios de terceros?	**[142]No procede** Se considera que la certificación ISO 27001 permite dar razonabilidad sobre la gestión de la seguridad de la información, por lo que, es un aspecto que las entidades deberán observar.	
	[143]ISACA c) certificación ISO 27001 vigente.	**[143]No procede** Ya está en la redacción.	
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.			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.			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.	**[144]BPDC** Existen servicios que por su naturaleza el respaldo está garantizado de acuerdo con el diseño de la solución y los componentes implementados, agregar un nuevo respaldo incrementa los costos y la administración.	**[144]No procede** Al final del inciso f) se indica: […]Lo anterior, cuando los servicios contratados, por su naturaleza, no garanticen o incluyan el respaldo.”	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			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.			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.	**[145]MUCAP** Con respecto al control de la administración de usuarios y privilegios, es importante que se amplie lo argumentado, ya que los accesos y privilegios a los servicios de los proveedores es muy propio de cada entidad.	**[145]No procede** Al final de la propuesta de artículo se indica que es "De conformidad con el modelo de servicio contratado".	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.	**[146]OPCCCSS** 2. En el punto i no es clara la necesidad de si el registro, monitoreo y alarmas de eventos de incidentes de seguridad debe estar bajo el dominio del supervisado o del proveedor del servicio.	**[146]No procede** Es responsabilidad de las entidades y empresas supervisadas velar por que se establezcan los controles técnicos y administrativos para la gestión y de usuarios y sus privilegios, indistintamente del proveedor del servicio.	i) Contar con sistemas de registro, monitoreo y alarma de eventos e incidentes de seguridad de la información y seguridad cibernética.
	[147]MUCAP Adicionalmente, establecer como obligación "Contar con sistemas de registro, monitoreo y alarma de eventos e incidentes de seguridad de la información y seguridad cibernética." se debe considerar el impacto financiero al elevarse los costos para las entidades a raíz de este requerimiento.	**[147]No procede** Para el cierre de las brechas que pueda tener la entidad en relación con las disposiciones del presente reglamento, se incluyó un transitorio séptimo.	
j) Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente.	**[148]MUCAP** En lo que respecta a "Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente." no existe la claridad de cómo se operativiza esta obligación ya que ante un tercero solo se podría dejar a nivel contractual la responsabilidad. Un ejemplo de ello es con relación a las multinacionales	**[148]No procede** Es responsabilidad de las entidades y empresas supervisadas velar por que se establezcan los controles técnicos y administrativos para el monitoreo de los servicios contratados.	j) Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente.

	donde el poder de negociación es muy bajo.		
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.	**[149]OPCCCSS** 3. En el punto k se menciona "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". ¿En qué casos aplicaría y hasta dónde debería llegar la aplicación de este control en la cadena de suministro?	**[149]No procede** Es responsabilidad de las entidades y empresas supervisadas velar por que se establezcan los controles técnicos y administrativos para el monitoreo del cumplimiento de los acuerdos y establecer el alcance en función de los riesgos.	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.
	[150]MUCAP Por otra parte, con relación a la obligación de "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.", surge la duda en los casos donde aplicaría y hasta dónde debería llegar la aplicación de este control en la cadena de abastecimiento.	**[150]No procede** Es responsabilidad de las entidades y empresas supervisadas velar por que se establezcan los controles técnicos y administrativos para el monitoreo del cumplimiento de los acuerdos y establecer el alcance en función de los riesgos.	
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.	**[151]CB** Inciso l): Con respecto al inciso l., se debe asegurar también que la empresa contratante del servicio tenga acceso a las llaves criptográficas de estos canales de comunicación.	**[151]No procede** Las entidades y empresas supervisadas deben establecer los controles técnicos de conformidad con su tamaño, complejidad, modelo de negocio y riesgos.	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			**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.			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			**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			**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.			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.	**[152]CAJAANDE** Cuando se indica que: " incluye a entidades y empresas integrantes de grupos y conglomerados financieros supervisados, o entidades y empresas del grupo económico", ¿esto únicamente aplicaría en caso de que la gestión de TI sea aceptada como corporativa?	**[152]No procede** No necesariamente es el caso planteado por la entidad, pues dicha responsabilidad corresponde también a las entidades y empresas integrantes de grupos y conglomerados financieros supervisados, o entidades y empresas del grupo económico.	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.			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 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.			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			**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.	**[153]BNCR** Se sugiere especificar cuál sería el alcance mínimo del análisis de riesgos que deben realizar las entidades para mantener identificados los riesgos de proveedores de bienes y servicios de TI críticos, para que haya un estándar mínimo de la aspiración del Regulador en esta materia, en atención a las mejores prácticas y el principio de proporcionalidad.	**[153] No procede** Las entidades y empresas supervisadas pueden utilizar estándares, marcos de referencia y buenas prácticas para la gestión de riesgos. La industria relacionada con TI ha desarrollado algunos como la ISO 31000, los procesos de CobiT 2019 para riesgos entre otras. Los cuales tienen dentro de sus prácticas las actividades de identificación de riesgos, establecimiento de contexto entre otras. Por lo que, es responsabilidad de las entidades y empresas supervisadas establecer los elementos mínimos de conformidad con su modelo de negocio, tamaño y complejidad.	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.
	[154]ABC El Reglamento debe especificar cuál sería el alcance mínimo del análisis de riesgos que deben realizar las entidades para mantener identificados los riesgos de proveedores de bienes y servicios de TI críticos. Lo anterior para tener claridad de cuál es la expectativa del regulador sobre este punto. De igual forma, es importante que se haga referencia a la aplicación del principio de proporcionalidad para tales efectos.	**[154] No procede** Las entidades y empresas supervisadas pueden utilizar estándares, marcos de referencia y buenas prácticas para la gestión de riesgos. La industria relacionada con TI ha desarrollado algunos como la ISO 31000, los procesos de CobiT 2019 para riesgos entre otras. Los cuales tienen dentro de sus prácticas las actividades de identificación de riesgos, establecimiento de contexto entre otras. Por lo que, es responsabilidad de las entidades y empresas supervisadas establecer los	

		elementos mínimos de conformidad con su modelo de negocio, tamaño y complejidad.	
	[155]CB Para los artículos 26 y 27, se sugiere especificar cuál sería el alcance mínimo del análisis de riesgos que deben realizar las entidades para mantener identificados los riesgos de proveedores de bienes y servicios de TI críticos, para que haya un estándar mínimo de la aspiración del Regulador en esta materia, en atención a las mejores prácticas y el principio de proporcionalidad.	**[155] No procede** Las entidades y empresas supervisadas pueden utilizar estándares, marcos de referencia y buenas prácticas para la gestión de riesgos. La industria relacionada con TI ha desarrollado algunos como la ISO 31000, los procesos de CobiT 2019 para riesgos entre otras. Los cuales tienen dentro de sus prácticas las actividades de identificación de riesgos, establecimiento de contexto entre otras. Por lo que, es responsabilidad de las entidades y empresas supervisadas establecer los elementos mínimos de conformidad con su modelo de negocio, tamaño y complejidad.	
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.			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			**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.	**[156]BNCR** Se sugiere especificar cuál sería el alcance mínimo del análisis de riesgos que deben realizar las entidades para mantener identificados los riesgos de proveedores de bienes y servicios de TI críticos, para que haya un estándar mínimo de la aspiración del Regulador en esta materia, en atención a las	**[156] No procede** Las entidades y empresas supervisadas pueden utilizar estándares, marcos de referencia y buenas prácticas para la gestión de riesgos. La industria relacionada con TI ha desarrollado algunos como la ISO 31000, los procesos	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.

	mejores prácticas y el principio de proporcionalidad.	de CobiT 2019 para riesgos entre otras. Los cuales tienen dentro de sus prácticas las actividades de identificación de riesgos, establecimiento de contexto entre otras. Por lo que, es responsabilidad de las entidades y empresas supervisadas establecer los elementos mínimos de conformidad con su modelo de negocio, tamaño y complejidad.	
	[157]ABC Es importante considerar la observación realizada al artículo 26 en torno a detallar cuál sería el alcance mínimo del análisis de riesgos y principio de proporcionalidad.	**[157] No procede** Las entidades y empresas supervisadas pueden utilizar estándares, marcos de referencia y buenas prácticas para la gestión de riesgos. La industria relacionada con TI ha desarrollado algunos como la ISO 31000, los procesos de CobiT 2019 para riesgos entre otras. Los cuales tienen dentro de sus prácticas las actividades de identificación de riesgos, establecimiento de contexto entre otras. Por lo que, es responsabilidad de las entidades y empresas supervisadas establecer los elementos mínimos de conformidad con su modelo de negocio, tamaño y complejidad.	
	[158]CB Para los artículos 26 y 27, se sugiere especificar cuál sería el alcance mínimo del análisis de riesgos que deben realizar las entidades para mantener identificados los riesgos de proveedores de bienes y servicios de	**[158] No procede** Las entidades y empresas supervisadas pueden utilizar estándares, marcos de referencia y buenas prácticas para la gestión de riesgos. La industria relacionada con TI ha desarrollado algunos	

	TI críticos, para que haya un estándar mínimo de la aspiración del Regulador en esta materia, en atención a las mejores prácticas y el principio de proporcionalidad.	como la ISO 31000, los procesos de CobiT 2019 para riesgos entre otras. Los cuales tienen dentro de sus prácticas las actividades de identificación de riesgos, establecimiento de contexto entre otras. Por lo que, es responsabilidad de las entidades y empresas supervisadas establecer los elementos mínimos de conformidad con su modelo de negocio, tamaño y complejidad.	
Artículo 28. Acuerdos de confidencialidad			**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.			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.			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			**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.	**[159]BPDC** 1-Valorar incluir en los contratos las evaluaciones a los proveedores para verificar los cumplimientos en materia de ciberseguridad y gestión de riesgos. 2-Además, incluir clausulas sobre la gestión de incidentes de seguridad de la información y ciberseguridad	**[159]No procede** 1-Lo indicado es una responsabilidad que está inmersa en la disposición de gestionar los contratos y los acuerdos de nivel de servicio del artículo. 2-Lo indicado está en la disposición relacionada con que los contratos y acuerdos de nivel de servicio deben contener cláusulas que aseguren la continuidad de los bienes y servicios de TI tercerizados.	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.	**[160]BNCR** Para el segundo párrafo se sugiere ajustar de la siguiente manera: "Los contratos y acuerdos de nivel de servicio deben contener cláusulas que aseguren la continuidad de los bienes y servicios de TI tercerizados. Así mismo, a la empresa o profesional independiente que realice la auditoría externa de TI, debe garantizar que su labor no interfiera con las operaciones para la prestación de los servicios de la entidad o empresa supervisada".	**[160]No procede** La regulación no puede establecer disposiciones a empresas y profesionales independientes porque no son regulados.	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.
	[161]CB Se sugiere ajustar el párrafo segundo de la siguiente manera: "Los contratos y acuerdos de nivel de servicio deben contener cláusulas que aseguren la continuidad de los bienes y servicios de TI tercerizados. Asimismo, a la empresa o profesional independiente que realice la auditoría externa de TI, debe garantizar que su labor no interfiera con las operaciones para la prestación de los servicios de la entidad o empresa supervisada".	**[161]No procede** La regulación no puede establecer disposiciones a empresas y profesionales independientes porque no son regulados.	
	[162]ISACA Los acuerdos deben contener cláusulas sobre la seguridad de la información y cibernética.	**[162]No procede** Lo indicado es algo que está inmerso dentro los aspectos que es necesario considerar para efectos de asegurar la continuidad de los bienes y servicios de TI críticos que son tercerizados. Por otra parte, en los lineamientos generales se establecen aspectos a considerar para la elaboración de los contratos y acuerdos, dentro de los cual, se hace referencia a aspectos de seguridad de la información y seguridad cibernética.	

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 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.			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			**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.	**[163]BPDC** Esta redacción se debe ajustar, ya que se debe definir el alcance, justificación, necesidad de acceso y estar en cumplimiento de regulaciones vigentes ley 8968 y ley9048.	**[163]No procede** La presente modificación reglamentaria se alinea con los dispuesto en las citadas leyes, por lo que no se contradicen. Las Superintendencias, para efectos de supervisión, solicitarán información dentro ámbito legal que faculta al supervisor.	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.
	[164]BCR Se solicita especificar como se tratan los casos en donde exista información confidencial que un tercero no puede revelar.	**[164]No procede** La presente modificación reglamentaria se alinea con lo dispuesto en las leyes 8968 y 9048, por lo que considera el tratamiento de los datos. Las Superintendencias, para efectos de supervisión, solicitarán información dentro ámbito legal que faculta al supervisor.	
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.			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			**CAPÍTULO IV**

SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD CIBERNÉTICA			**SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD CIBERNÉTICA**
Sección I. Gestión de la seguridad de la información y la 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			**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.	**[165]BPDC** Se debe clarificar si el SGSI debe ser certificado o no, en caso de requerirlo dar tiempo prudencia	**[165] No procede** En ningún caso el marco de regulación hace referencia a que la entidad deba certificarse o deba certificar algún proceso de TI. Las decisiones de certificar el SGSI, queda a discreción de cada entidad o empresa supervisada en función de su estrategia de negocio.	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.	**[166]COOPEFYL** ¿Según el Acuerdo Sugef 25-23 las cooperativas de regulación proporcional se eximen de la administración de riesgos, como se atiende este requerimiento.? Para establecer la Declaración de aplicabilidad se requiere de una evaluación de riesgos que permita guiar los controles que se ejecutarán por lo tanto debe disponerse de una metodología de administración de riesgos, lo cual el acuerdo Sugef 25-23 exime a algunas cooperativas	**[166]No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que	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.

		discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, la afirmación de Coopefyl no es correcta respecto a que se eximió a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
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.			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.	**[167]BAC** Se solicita evaluar la redacción del último párrafo del Artículo 31. Sistema de gestión de la seguridad de la información. Se considera que los controles se deben incluir por que obedecen a riesgos identificados. No por supervisión	**[167]Procede** Se ajusta la redacción.	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 l~~a~~os ~~necesidades de supervisión y el~~ riesgos identificados.
Artículo 32. Seguridad cibernética			**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.	**[168]BPDC** Considerar cambiar Seguridad Cibernética por Ciberseguridad. ¿El concepto de resiliencia operativa digital se refiere a la continuidad de negocio o a la continuidad de TI?	**[168]No procede** Como se evidencia en el documento del Financial Stability Board (FSI) titulado "Cyber Lexicon" y en el documento de ISACA denominado "Glosario de Términos y Definiciones", ambos términos pueden emplearse de manera equivalente.	Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital.

		Seguridad Cibernética y Ciberseguridad se utilizan de forma indistinta, para efectos del presente Reglamento se utiliza seguridad cibernética.	
	[169]BNCR Se comprende que este reglamento hace alusión a la seguridad de la información y se pide el establecimiento de un sistema de gestión de seguridad de la información; sin embargo, se observa que dentro de los elementos de control se enfocan en la seguridad cibernética únicamente, dejando de lado un tema muy importante: la seguridad física de las instalaciones físicas e infraestructuras que apoyan la gestión operativa del negocio y específicamente la gestión de TI, por lo que se considera relevante que se valore la inclusión de esos elementos en el presente reglamento.	**[169] No procede** Este artículo trata únicamente sobre la seguridad cibernética. En el Acuerdo SUGEF 2-10 se hace referencia a todo lo relacionado con gestión de riesgo operativo, donde se considera lo referente a seguridad física.	
	[170]CB Se comprende que este reglamento hace alusión a la seguridad de la información y se pide el establecimiento de un sistema de gestión de seguridad de la información; sin embargo, se observa que dentro de los elementos de control se enfocan en la seguridad cibernética únicamente, dejando de lado un tema muy importante: la seguridad física de las instalaciones físicas e infraestructuras que apoyan la gestión operativa del negocio y específicamente la gestión de TI, por lo que se considera relevante que se valore la inclusión de esos elementos en el presente Reglamento.	**[170] No procede** Este artículo trata únicamente sobre la seguridad cibernética. En el Acuerdo SUGEF 2-10 se hace referencia a todo lo relacionado con gestión de riesgo operativo, donde se considera lo referente a seguridad física.	

Las entidades y empresas supervisadas deben establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética.	**[171]BAC** Se solicita evaluar la redacción del último párrafo del Artículo 32. Seguridad cibernética. Se considera que el tema de eficacia y eficiencia es algo que se decide cuando se plantean los controles y planes de acción para darle tratamiento a los riesgos identificados.	**[171]No procede** Evaluar el rendimiento cibernético de la organización es una de las claves para garantizar que los activos y datos informáticos (tanto sensibles como no sensibles) están protegidos, y que los clientes y partes interesadas confían en la entidad.	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			**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.	**[172]ABC** La norma debería ejemplificar las pruebas que se consideran adecuadas.	**[172]No procede** La gestión de riesgos debe realizarse de forma integral en la organización, por lo tanto, es la entidad la que debe establecer en función de su modelo de negocio, complejidad, tamaño y los riesgos asociados a su plataforma tecnológica, el alcance de los análisis y pruebas de vulnerabilidades.	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 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.			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			**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.	**[173]BPDC** Se debe sugerir donde deberían estar ubicados o reportar estas unidades, funciones, centros de operación y comités.	**[173]No procede** Es responsabilidad de las entidades y empresas supervisadas establecer unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen los riesgos de la	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.

		seguridad cibernética. Adicionalmente, el Articulo 8 indica que el Órgano de dirección es el responsable de aprobar las estructuras necesarias para la implementación del marco de gobierno y gestión de TI.	
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 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.			Las unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen~~s~~ 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.			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			**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.			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.	**[174]COOPEFYL** Excluyeron proveedores, pero dejaron partes interesadas, este término podría incluir proveedores.	**[174]Procede** Se ajusta la redacción.	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~~,~~ y clientes ~~y demás partes interesadas~~.
Los planes deben contener indicadores de medición para determinar el nivel de concientización de las entidades o empresas supervisadas.			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			**Sección II. Incidentes de seguridad de la información y seguridad cibernética**

Artículo 36. Gestión de 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.			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.			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.			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			**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.			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.	**[175]OPCCCSS** En el párrafo "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" Considerar involucrados claves ante un incidente	**[175]No procede** La expectativa de las Superintendencias es que sean las entidades las que definan dentro de su organización las personas que consideran clave dentro de su función de respuesta a incidentes de seguridad de la información y seguridad cibernética.	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:			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.			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.	**[176]BPDC** Los elementos de este punto b deben estar definidos y alineados con la ley 8968	**[176]No procede** A fin de cumplir con la legislación nacional aplicable a las entidades, así como garantizar la privacidad y la seguridad de la información personal de los individuos, las entidades deben cumplir con lo dispuesto en la Ley 8968. Esta ley establece las obligaciones que deben cumplir las organizaciones que recopilan, almacenan o procesan datos personales, así como los derechos que tienen las personas sobre sus datos.	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.			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.			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.			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			**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.	**[177]OPCCCSS** Respecto al párrafo "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". No queda claro, si desean que separemos las situaciones	**[177] No procede** En los lineamientos generales de la presente modificación reglamentaria se encuentra la tabla de clasificación para el registro de los incidentes de seguridad de la información y seguridad cibernética. Asimismo, dichos lineamientos contienen la tabla de clasificación del impacto de los citados incidentes.	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.

	de riesgo (eventos / incidentes); en los que son de Seguridad de la Información y otros de Seguridad Cibernética. Esto llevaría hacer grandes cambios en el tratamiento de riesgos materializados, ya que tenemos la división entre casos Operativos y de SI. Incluso considerar que riesgos de seguridad cibernética, están generalmente relacionados con Seguridad de la Información.	En el caso de las entidades supervisadas por SUGEF, estas ya remiten mediante el reporte de riesgo operativo los incidentes.	
Artículo 39. Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias			**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".	**[178]ABC** El regulador está obligando a las entidades a remitir informes durante la fase de "detección y análisis" y de "contención, mitigación y recuperación". La imposición de este deber, en estas etapas, obliga a las entidades a destinar recursos importantes que se requieren precisamente para atender estas etapas. Si bien la oportunidad de la información es importante, la inmediatez que propugna la reforma (8 horas según los lineamientos) podría replantearse para que no sea concomitante con el desarrollo del incidente, y, además, para ajustarse a los estándares internacionales. Por otro lado, se requiere de mayor precisión de la graduación de los impactos para poder determinar qué se considera un impacto moderado o alto.	**[178]No procede** La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad. La propuesta de modificación regulatoria hace referencia a que la entidad remita a la respectiva Superintendencia un comunicado inicial, el cual, servirá para valorar el impacto que tiene el evento y posibles pasos a seguir por parte de las Superintendencias para el monitoreo de las acciones a ejecutar por parte de la entidad. Las entidades y empresas supervisadas definirán el contenido mínimo del comunicado, considerando que este sea oportuno, claro y con un alcance apropiado en función del incidente.	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".
	[179]CB Se sugiere la valoración de un ajuste en la redacción, ya que durante la fase	**[179]No procede** La propuesta reglamentaria contiene las expectativas que las	

	de "detección y análisis" no se tiene certeza absoluta de que se trate de un incidente y se podría producir una falsa alarma innecesariamente. Por otro lado, durante la fase de "contención, mitigación y recuperación" es mejor que la entidad o empresa supervisada centre su atención y recursos en la solución del incidente, de manera que una vez solucionado, pueda tener claridad de lo acontecido y así elaborar y emitir los informes correspondientes. Este no es un tema menor, por lo que se solicita la valoración respectiva, considerando la práctica y la realidad en esta materia. El mismo Regulador ha experimentado incidentes que no le es posible explicar a los supervisados en esas fases, por su misma naturaleza, por lo que se estima necesario su consideración al respecto.	superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Por otra parte, se modificó la redacción del artículo considerando parte de lo indicado en la observación y se realizaron los ajustes para las salvedades en los lineamientos. Se espera que, en la fase de detección y análisis, una vez que la entidad o empresa supervisada ha hecho el triage respectivo, comunique el incidente a la respectiva Superintendencia.	
Las Superintendencias podrán solicitar informes sobre la atención de los incidentes de seguridad de la información o de seguridad cibernética.			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.			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.			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			**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			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.			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.	**[180]COOPEFYL** Porque es un plazo tan alto, aquí se está dejando desprotegidos a los clientes, debe reducirse el mismo, y los impactos que genera para los clientes no interesa. Debe dejarse 2 días como estaba en la anterior consulta. ¿Según el Acuerdo Sugef 25-23 las cooperativas de regulación proporcional se eximen de la administración de riesgos, como se atiende este requerimiento?	**[180]No procede** A partir de diversas observaciones recibidas como parte del proceso de la primera consulta externa, se consideró que dos días no es viable, dados los protocolos internos de escalamiento, por lo que se consideró razonable establecer el plazo de cinco días. Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno corporativo, idoneidad y administración de riesgos no serán objeto de supervisión ni de evaluación por parte de la Superintendencia. Asimismo, indica que, dichas disposiciones no serán de cumplimiento obligatorio, sino que, las entidades que así los dispongan, pueden adoptar dichas disposiciones como referencias sobre sanas prácticas. De manera consistente con lo anterior, en el artículo 3. Regulación proporcional, se indica que, lo dispuesto en los capítulos: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información; se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus	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.

		riesgos, tamaño, complejidad y modelo de negocio. Por lo tanto, no se exime a un grupo de cooperativas de implementar aspectos de gobierno corporativo y de gestión de riesgos, ya que, la regulación no indica que queda a la libre; la regulación hace referencia que la entidad con base en las referencias de sanas prácticas defina su marco de gobierno y gestión de riesgos.	
	[181]CB Se solicita especificar como tratar las violaciones de la privacidad de los datos personales según la ley 8968.	**[181]No procede** Este es un tema que está fuera del alcance de esta regulación. Esta norma ya establece el tratamiento de los incidentes que impactan aspectos de datos personales. A fin de cumplir con la legislación nacional aplicable a las entidades, así como garantizar la privacidad y la seguridad de la información personal de los individuos, las entidades deben cumplir con lo dispuesto en la Ley 8968. Esta ley establece las obligaciones que deben cumplir las organizaciones que recopilan, almacenan o procesan datos personales, así como los derechos que tienen las personas sobre sus datos. Por lo tanto, las entidades y empresas supervisadas deberán establecer los respectivos controles administrativos y técnicos.	
Artículo 41. Reporte histórico de incidentes de seguridad de la información y seguridad cibernética			**Artículo 41. ~~Reporte~~ Información histórico~~a~~ 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.	**[182]OPCCCSS** No indica la periodicidad del reporte, si queda sujeto a la definición por parte de la entidad supervisada. Es importante establecer un procedimiento para generarlo de forma ágil cuando este se requiera.	**[182]Procede** Se modifica la redacción para hacer referencia a un plazo de conservación de la información histórica de incidentes de seguridad de la información y seguridad cibernética. Dicho plazo se define en los lineamientos, para lo cual, se tomó como referencia de sana práctica el plazo de conservación de archivos dispuesto en la Ley del Sistema Nacional de Archivos.	Las entidades y empresas supervisadas deben ~~elaborar un reporte~~ mantener información histórico~~a~~ de los incidentes de seguridad de la información y seguridad cibernética. ~~El reporte~~ La información histórica 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 de~~l reporte~~ la información.
	[183]ABC No se especifica por cuánto tiempo se debe conservar el reporte "histórico de incidentes" ni cuánto tiempo atrás puede, el supervisor, solicitar la información histórica de incidentes.	**[183]Procede** Se modifica la redacción para hacer referencia a un plazo de conservación de la información histórica de incidentes de seguridad de la información y seguridad cibernética. Dicho plazo se define en los lineamientos, para lo cual, se tomó como referencia de sana práctica el plazo de conservación de archivos dispuesto en la Ley del Sistema Nacional de Archivos.	
El contenido del reporte está establecido en los lineamientos generales del presente reglamento.			El contenido y el plazo de conservación de~~l reporte~~ la información histórica 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.			~~Las Superintendencias comunicarán los canales de remisión del reporte histórico de los incidentes de seguridad de la información y seguridad cibernética.~~
CAPÍTULO V			**CAPÍTULO V**
LA AUDITORÍA EXTERNA DE TI			**LA AUDITORÍA EXTERNA DE TI**
Sección I. Perfil tecnológico			**Sección I. Perfil tecnológico**
Artículo 42. Perfil tecnológico			**Artículo 42. Perfil tecnológico**
Las entidades y empresas supervisadas deben elaborar su perfil tecnológico y actualizarlo anualmente.			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,			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.			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.			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.	**[184]COOPEFYL** Se están valorando inicialmente los cambios en perfil, pero esto conlleva a trabajos con proveedores externos por lo que se debe considerar un plazo prudencial para poder cumplir con estos cambios en el perfil y ¿Cuándo van a publicar los cambios a los XML del perfil tecnológico?	**[184]No procede** En la disposición transitoria sexta, se indica que, por el momento, 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. Por lo que, se estarán habilitando espacios para realizar los ajustes y pruebas correspondientes en su debido momento.	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			**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.	**[185]COOPEFYL** Las cooperativas que estamos en regulación proporcional ya se definen los procesos aplicables en el Anexo No. 2, no hay claridad si ¿el requisito del Estudio Técnico para justificar los procesos son o no aplicables?	**[185]No procede** En el artículo 3. Regulación proporcional, se indica que para las entidades sujetas al Acuerdo SUGEF 25-23, no es de aplicación lo dispuesto en el artículo 43.	Las entidades y empresas supervisadas deben indicar en el perfil tecnológico cuáles de los procesos de evaluación detallados en el anexo 1 de 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.
	[186]OPCCCSS	**[186]No procede**	

	1. Aclarar si los procesos que conforman el Marco de Gobierno y de Gestión de TI se podrán implementar con un nivel de capacidad específico (el sugerido) y si la evaluación por parte de los auditores se realizaría con base en dicho nivel o basada en riesgos. Esto dado que, en el Anexo de los procesos solamente viene la descripción y propósito de cada uno, y en la matriz de evaluación se incluyen las prácticas de gestión / gobierno, pero no se sabe qué nivel o cuáles actividades deben implementarse como tal. 2. Se menciona que, "los procesos de evaluación que no les apliquen deben estar debidamente fundamentados en un estudio técnico, el cual debe ser remitido mediante los canales oficiales de comunicación de cada Superintendencia. Los aspectos que deben ser considerados para la elaboración del estudio técnico están establecidos en los lineamientos generales del presente reglamento". Sin embargo, a las empresas con regulación proporcional ya se les definieron los procesos aplicables, según el Anexo 2 de los Lineamientos Generales. Por favor aclarar si para estas entidades es o no necesario el requisito del estudio técnico para justificar los procesos no aplicables.	1-En materia de implementación, es algo que queda a criterio de la entidad. Las Superintendencias no establecen un nivel de capacidad para la implementación de las prácticas de gobierno y gestión comúnmente aceptadas a nivel internacional. Queda a discreción de las entidades y empresas supervisadas utilizar este criterio o bien implementarlas de conformidad con el modelo de negocio, tamaño, complejidad de las operaciones y los riesgos. 2-En el artículo 3. Regulación proporcional, se indica que para las entidades sujetas al Acuerdo SUGEF 25-23, no es de aplicación lo dispuesto en el artículo 43.	
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.			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.			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.			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.			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			**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.	**[187]ISACA** No incluyeron el anexo para valorar la asociación	**[187]No procede** Los anexos están en los lineamientos generales de la presente modificación reglamentaria.	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.			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			**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.	**[188]ABC** No está claro qué debe entenderse por "cambio significativo", lo cual es fundamental para reducir la subjetividad al momento de aplicar la presente disposición.	**[188]Procede** Las entidades son las que establecerán los cambios que son considerados significativos. Por otra parte, se modifica la redacción para mejorar el entendimiento.	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 en aspectos tales como impacto en: la operación, la seguridad, el cumplimiento, la inversión requerida, los beneficios esperados, el alcance de los

		Se ejemplifican algunos ejemplos de lo que podría conllevar un cambio significativo.	procesos de evaluación aplicables a la entidad, los riesgos asociados y su alineación con la estrategia organizacional, entre otros. 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.			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			**Sección II. Auditoría externa de TI**
Artículo 46. 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.	**[189]OPCCCSS** Es importante que cuando el Supervisor solicite la Auditoría Externa de TI, detalle de forma concisa y clara el alcance, en otras ocasiones establecieron la revisión de todos los sistemas y esto al ser ambiguo, ocasionó que los servicios de estas auditorias se cotizaran por encima de los 150 mil dólares, generando atrasos por la falta de identificación clara del alcance.	**[189]Procede (comentario)** Como parte de la práctica supervisora, las Superintendencias solicitarán a las entidades y empresas supervisadas la coordinación de reuniones previo a la contratación del auditor externo de TI, para aclarar las expectativas de los alcances de las auditorías externas requeridas por las Superintendencias.	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
	[190]ISM Las Superintendencias solicitarán a las entidades y empresas supervisadas la contratación de una auditoría externa de TI sobre el Sistema de gobierno y gestión de TI.	**[190]No procede** Se prefiere el término de “marco de gobierno y gestión de TI”, el cual, es el utilizado por las Superintendencias y es homólogo al sistema de gobierno y gestión de TI a que hace referencia CobiT. El "sistema de gobierno y gestión de TI" se enfoca en la estructura y las actividades operativas diarias relacionadas con la TI dentro de una organización, el "marco de gobierno y gestión de TI" proporciona las directrices y metodologías más amplias para guiar y controlar el uso estratégico	

		y operativo de la tecnología de la información. Por lo tanto, el término "marco" está más alineado con los fines regulatorios, mientras que el término sistema se relaciona más con la implementación.	
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.			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.	**[191]BCR** En contratos de suscripción no es posible solicitarle al proveedor una auditoría externa, a una empresa que no está sujeta a esta regulación.	**[191]No procede** Las autoridades de regulación locales conocen lo comentado respecto a la dificultad de solicitar auditorías externas a proveedores mediante contratos de adhesión o suscripción, como es el caso de los proveedores de servicios de computación en la nube, por lo cual, se admite que, en el caso de proveedores reconocidos internacionalmente de estos servicios, las Superintendencias podrán valorar la aceptación de dichos informes de auditoría que estén a disposición por parte de dichos proveedores.	Cuando las entidades y empresas supervisadas dispongan de sus componentes tecnológicos mediante el uso de servicios de computación en la nube proveídos por terceros o se celebren contratos de adhesión, las Superintendencias podrán valorar la aceptación de informes de auditorías externas con las que ya cuenten dichos proveedores.
	[192]CB En contratos de suscripción, no es posible solicitarle que realice una auditoría externa, a una empresa que no está sujeta a esta regulación.	**[192]No procede** Las autoridades de regulación locales conocen lo comentado respecto a la dificultad de solicitar auditorías externas a proveedores mediante contratos de adhesión o suscripción, como es el caso de los proveedores de servicios de computación en la nube, por lo cual, se admite que, en el caso de proveedores reconocidos internacionalmente de estos servicios, las Superintendencias	

		podrán valorar la aceptación de dichos informes de auditoría que estén a disposición por parte de 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.	**[193]ISACA** Considerar que el auditor externo además de ser CISA tenga acreditación en fundamentos de Cobit	**[193]Procede** Las acreditaciones están establecidas en el Reglamento General de auditores externos, Acuerdo Conassif 1-10. Por lo que, es un aspecto que podrá ser valorado en el futuro. Sin embargo, el principal requisito para los auditores externos de TI es la certificación CISA de ISACA, la cual, a su vez, requiere formación y capacitación continua de los profesionales acreditados.	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 cuentean 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.	**[194]COOPEFYL** ¿Deben estar registrados en las bases de datos de SUGEF como auditores externos autorizados?	**[194]No procede** En el artículo 3. Auditoría externa del Reglamento General de Auditores Externos, Acuerdo Conassif 1-10, se indica que, las auditorías deben estar a cargo, exclusivamente, de firmas de auditoría externa o auditores externos independientes, inscritos en el Registro de Auditores Externos que forma parte del Registro Nacional de Valores e Intermediarios, dispuesto en la Ley Reguladora del Mercado de Valores. Además, que la Superintendencia General de Valores será la responsable de la gestión del 'Registro de Auditores Externos' que se define en el Acuerdo Conassif 1-10.	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			**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:			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.			a) Los procesos de evaluación del marco de gobierno y gestión de TI establecidos en los anexos 1 y 2 de los lineamientos generales del presente reglamento, aplicables a la entidad en el momento de la solicitud de la auditoría externa de TI, de conformidad con los artículos 3 y 43 del presente reglamento.
b) Las funciones para la evaluación de la gestión de riesgos de seguridad cibernética establecidas en los lineamientos generales del presente reglamento.			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.			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.			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.			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.	**[195]SAGICOR** En cuanto al punto e. Si esta superintendencia solicitara auditar también a los proveedores de TI en los procesos que se soliciten, se solicita a esta superintendencia, tomar en consideración que esto podría no ser posible para proveedores con contratos de adhesión como es el caso de Sales Force por ejemplo, y de los cuales es la mayoría de proveedores de servicios de nube, en algunos otros casos, la petición de auditoría a proveedores locales pero externos, podría incluir costos que el contrato no contempla, tiempos que podrían exceder los 9 meses, e incluso los posibles resultados, no son	**[195]No procede** La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Además, es común que los más reconocidos proveedores de servicios de computación en la nube ya cuenten con informes de auditorías externas, por lo que, en esos casos, tal como lo indica el artículo, las Superintendencias podrán valorar la aceptación de dichos informes de auditoría.	f) El periodo de cobertura.

	necesariamente vinculantes al proveedor. Les solicito amablemente analizar detenidamente los casos donde sea necesario aplicarlo y si lo creen necesario reescribir el artículo.	Se agregó: "o con contratos de adhesión" en el artículo 46. En la Sección V. Lineamientos relacionados con el diseño de los contratos y acuerdos de nivel de servicio, ubicada en los lineamientos generales se indica la habilitación que debe tener la entidad para solicitar este tipo de auditorías a los proveedores. Los aspectos de costo y de plazo es necesario dimensionarlos en función de la criticidad de los servicios suministrados por el proveedor.	
g) Aspectos que las Superintendencias requieran de conformidad con los riesgos identificados.			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.			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.	**[196]BCR** Considerar adecuar el plazo de ejecución al alcance de los requerimientos solicitados en la auditoría externa, dado que los alcances de la auditoría externa con cada iteración se van ampliando, sin embargo, se sigue manteniendo el plazo de 9 meses.	**[196]No procede** La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Cabe señalar que, las entidades podrán solicitar una prórroga para el envío de los productos de la auditoría externa, lo cual, deberá ser debidamente justificado.	El plazo para la auditoría externa de TI y los canales de remisión del alcance están establecidos en los lineamientos generales del presente reglamento.
	[197]CB	**[197]No procede**	

	Se solicita adecuar el plazo de ejecución, dado que los alcances de la auditoría externa con cada iteración se van ampliando, sin embargo, se sigue manteniendo el plazo de 9 meses.	La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Cabe señalar que, las entidades podrán solicitar una prórroga para el envío de los productos de la auditoría externa, lo cual, deberá ser debidamente justificado.	
Artículo 48. Periodicidad de las auditorías externas de TI			**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.	**[198]COOPEFYL** Deberían extender el plazo a 5 años, para las cooperativas que nos rige la Proporcionalidad de la SUGEF 25-23.	**[198]No procede** De conformidad con las expectativas de las Superintendencias, se considera prudente mantener la periodicidad de cada tres años. No obstante, las Superintendencias podrán valorar aquellos casos en que se considere según la supervisión basada en riesgo el hecho de aplazar la auditoría externa.	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.
	[199]VIDAPLENA En relación con el artículo 48, se les solicita aclarar a partir de que fecha se consideran los tres años, esta aclaración podría ser mediante un transitorio y para aquellas empresas que tienen o están finalizando la implementación de su MGTI; en este caso, si el plazo se estaría contando a partir de la entrega de la última auditoría externa de TI realizada o a partir de aprobado este reglamento. Lo anterior se señala, dado que la última auditoria de TI para esta operadora se entregó al Ente Supervisor en julio de 2022.	**[199]No procede** Las disposiciones de la modificación regulatoria entrarán en vigor a partir de su publicación en el diario oficial La Gaceta. Sin embargo, se incluye una disposición transitoria primera, en la cual, se indica que, 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. Además, las auditorías externas servirán, entre otras cosas, para	

	Lo anterior se consulta, también considerando lo señalado en el transitorio séptimo de este Reglamento, la referencia a "no mayor a tres años" para cerrar los planes de implementación, pareciera que está enfocada principalmente en lo solicitado en este reglamento, aunque se sobrentiende que una vez pasado los tres años en la Implementación de las modificaciones reglamentarias se realizará una auditoría externa de TI para asegurar que dicho reglamento se cumpliese, pero para el caso de esta operadora ya habrían pasado alrededor de cinco años desde nuestra última auditoría externa de TI, si fuese así como se está considerando.	conocer el avance que están teniendo las entidades respecto al cierre de brechas identificadas a parir de la entrada en vigor de las modificaciones regulatorias.	
	[200]ISTMO Evaluar que las auditorías sean en un plazo de cada 4 años, lo anterior se fundamenta en que los ciclos de auditoría y remediación a través de planes de acción pueden tomar hasta 2 años por lo que tener ciclos de auditoría cada 3 años es un proceso muy fuerte por otra parte la implementación de los marcos de gobierno corporativo y gestión de riesgos ya son temas hoy en día robustos y que plantean ciclos de mejora continua que vienen a asegurar el tratamiento de riesgos de seguridad de la información y seguridad cibernética, así como el mismo marco de gestión de TI.	**[200]No procede** De conformidad con las expectativas de las Superintendencias, se considera prudente mantener la periodicidad de cada tres años. No obstante, las Superintendencias podrán valorar aquellos casos en que se considere según la supervisión basada en riesgo el hecho de aplazar la auditoría externa.	
	[201]SAGICOR En ocasiones, debido a las extensiones de los planes de acción a los supervisados, la sumatoria de tiempo de los procesos de auditoría + los	**[201]No procede** De conformidad con las expectativas de las Superintendencias, se considera prudente mantener la periodicidad	

	procesos de aprobación de planes de acción + la ejecución de los planes de acción(incluidos los seguimientos), podrían alcanzar fácilmente los 3 años, si por motivos fuera de nuestro control, se ejecutan nuevas auditorías al cabo de la finalización de los planes de acción, la aseguradora/departamentos de TI se vería forzado a entrar permanente en auditorías y planes de acción, lo que limita grandemente el rango de acción para los otros compromisos que el mismo departamento tiene con esta superintendencia y con las metas de negocio, además ya está superintendencia ejerce marcos de supervisión y auditorías de riesgos que de manera indirecta ya mide temas que son adyacentes o similares, es decir ya contamos con otras auditorías que ayudan a que los entornos se mantengan seguros. Les solicito respetuosamente analizar la posibilidad de que los plazos de auditoría sean de 4 años mínimo, con el fin de que contar con el tiempo necesario para la estabilización y puesta en marcha de los procesos una vez finalizados los planes de acción en fin de evitar potenciales desgastes de los equipos. Gracias.	de cada tres años. No obstante, las Superintendencias podrán valorar aquellos casos en que se considere según la supervisión basada en riesgo el hecho de aplazar la auditoría externa.	
	[202]POPULARPENSIONES En vista de que el periodo de ejecución de la Auditoría Externa es de 9 meses, y adicionalmente se deben realizar presentaciones y planes de acción, es importante establecer el punto de partida. Se propone indicar cada tres años a partir de la aprobación por parte	**[202]No procede** De conformidad con las expectativas de las Superintendencias, se considera prudente mantener la periodicidad de cada tres años. No obstante, las Superintendencias podrán valorar aquellos casos en que se considere según la supervisión basada en	

	de la Superintendencia de los Planes de Acción correspondientes.	riesgo el hecho de aplazar la auditoría externa. Por otra parte, 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, por lo que no en todos los casos aplica lo sugerido en la observación.	
Artículo 49. Documentación sobre la contratación y la planificación de la auditoría externa de TI			**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:			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			a) la copia del contrato suscrito por los servicios de auditoría, y
b) la planificación del encargo.			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.			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			**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:			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.			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.			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.	**[203]COOPEFYL** ¿Cuándo nos darán la matriz de evaluación nueva acorde a reguladas por la proporcionalidad de la SUGEF 25-23 y si la misma incluye los niveles de capacidad en las actividades de	**[203]No procede** Respecto a la matriz de evaluación, en los lineamientos generales de la propuesta de modificación regulatoria se establece que las	c) La matriz de evaluación del marco de gobierno y gestión de TI.

	acuerdo al volumen y tamaño de la entidad?	Superintendencias pondrán a disposición de las entidades y empresas supervisadas, así como de los auditores externos de TI, la versión vigente de la herramienta que contiene la Matriz de evaluación del marco de gobierno y gestión de TI, así como las respectivas guías para su uso a través de los sitios electrónicos oficiales de cada Superintendencia. Además, se establece que, las "prácticas de gobierno y gestión" establecidas en la matriz de evaluación serán adoptadas y adaptadas por las entidades y empresas supervisadas de conformidad con sus riesgos identificados.	
	[204]ISACA Deben revisar la calificación del proceso (fuerte, aceptable, mejorable, débil). El color amarillo de aceptable tiende a la confusión, ya que denota que es un proceso regular, no de cumplimiento adecuado. El aceptable debería cambiarse a un término como "bueno", ser verde y el Fuerte azul	**[204]Procede** Se ajusta la matriz de evaluación según lo sugerido.	
d) Cualquier otro producto solicitado por la Superintendencia en el alcance de la auditoría externa 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.			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			**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	**[205]BCR** Se solicita valorar el plazo para enviar el Reporte de Supervisión, dado que las mejoras que resulten del informe	**[205] No procede** Este es un plazo máximo que está en función de la complejidad de los hallazgos en la entidad.	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.	de la auditoría externa podrían impactar el Plan Estratégico de la entidad además del Plan Estratégico de TI, además de los costos de contratación del auditor externo		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.			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			**Sección III. Reporte de supervisión y plan de acción**
Artículo 52. Reporte de supervisión			**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.			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.	**[206]CB** Se solicita mantener el plazo de 20 días hábiles que tienen actualmente las Superintendencias para enviar el Reporte de Supervisión, dado que las mejoras que resulten del informe de la auditoría externa podrían impactar el Plan Estratégico de la entidad además del Plan Estratégico de TI, además de los costos de contratación del auditor externo.	**[206] No procede** Este es un plazo máximo que está en función de la complejidad de los hallazgos en la entidad.	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.			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			**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.	**[207]BCR** 1-Cuáles son los aspectos mínimos por los que se determina que un producto no es admisible. 2-Conceder 10 días hábiles para ampliar un producto que fue construido en un plazo de 9 meses no	**[207]No procede** 1-En el artículo 52 de la propuesta de modificación regulatoria se indican los productos de la auditoría externa de TI. Además, se indica que, los formatos, características y canales de	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.

	es acorde con el alcance de lo auditado. Además, considerar el proceso de actualización, y aprobación de los diferentes equipos operativos, y órganos de dirección	remisión de los productos de la auditoría externa de TI están establecidos en los lineamientos generales del presente reglamento. Por lo tanto, el supervisor puede declarar inadmisibles los productos de la auditoría externa de TI cuando incumplan las disposiciones establecidas en el reglamento, en sus lineamientos generales o en ambos. 2-Este plazo de diez días es en caso de cambios menores que no requieran los 30 días.	
	[208]CB Se solicita aclarar cuáles son los aspectos mínimos por los que se determina que un producto no es admisible. Además, conceder 10 días hábiles para ampliar un producto que fue construido en un plazo de 9 meses no es acorde con el alcance de lo auditado. Resulta necesario, considerar el proceso de actualización y aprobación de los diferentes equipos operativos y órganos de dirección.	**[208]No procede** 1-En el artículo 52 de la propuesta de modificación regulatoria se indican los productos de la auditoría externa de TI. Además, se indica que, 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. Por lo tanto, el supervisor valorará cada caso y podrá declarar inadmisibles los productos de la auditoría externa de TI cuando incumplan las disposiciones establecidas en el reglamento, en sus lineamientos generales o en ambos. 2-Este plazo de diez días es en caso de cambios menores que no requieran los 30 días.	
	[209]ISACA Considerar que los funcionarios fiscalizadores de la supervisora deben ser también CISA y contar al menos con la acreditación de Cobit, para tener	**[209]No procede** En relación con CISA, se considerará para posibles análisis de estructuras organizacionales.	

	igual de condiciones en la valoración de la calidad de los productos de la auditoría.	Lo referente a Cobit forma parte de los perfiles de puesto.	
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.			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.	**[210]OPCCCSS** Se indica que "El plazo dispuesto para que las Superintendencias remitan nuevamente el reporte de supervisión iniciará a partir de la última recepción de los productos corregidos", se sugiere indicar cuántos días después estarían remitiendo nuevamente dicho reporte de supervisión para que la empresa esté enterada y planifiquen actividades a nivel interno considerando esas fechas. Además, considerar que ante el caso de inadmisibilidad, las entidades supervisadas deben fundamentar de forma técnica, el por qué se alejan de la opinión de un auditor externo certificado y las implicaciones a nivel de pedir el cambio de una opinión de un auditor acreditado en el colegio respectivo.	**[210] Procede** EL articulo 52 indica los plazos en los que la Superintendencia podrá remitir el reporte de supervisión. Por su parte, en este artículo 53, la disposición indica que el plazo dispuesto para que las Superintendencias remitan nuevamente el reporte de supervisión iniciará a partir de la última recepción de los productos corregidos. Se modifica la redacción para aclarar.	El plazo dispuesto en el artículo 52 del presente reglamento para que las Superintendencias remitan ~~nuevamente~~ el reporte de supervisión, iniciará nuevamente 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.			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			**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			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.			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.			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.	**[211]OPCCCSS** Se sugiere incluir un periodo de tiempo para que el supervisor indique si está de acuerdo o no con el plan de acción, para tener estimado cuándo se podría empezar a implementar el plan sin ningún problema.	**[211]No procede** 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, por lo que no en todos los casos aplica lo sugerido en la observación; va a depender de lo dispuesto por 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.	**[212]BCR** El plazo de elaboración del plan de acción debería ampliarse al menos a 40 días hábiles, dado que cuando la Gestión de TI es Corporativa, la elaboración del plan de acción requiere de la participación de todas las áreas (Banco y Subsidiarias) involucradas en las acciones que se definan, mismas áreas, que además deben atender su día a día, revisión y análisis de impacto en planes estratégicos, operativos y tácticos, sumado el tiempo de aprobación en los diferentes órganos de dirección (Comité Corporativo Ejecutivo, Comité Corporativo de TI, Juntas Directivas).	**[212] No procede** El plazo dispuesto en el artículo se estableció de conformidad con lo establecido en otras normas vigentes aprobadas por el CONASSIF, las cuales, consideran la elaboración de planes de acción.	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.
	[213]CB El plazo de elaboración del plan de acción debería ampliarse al menos a	**[213] No procede** El plazo dispuesto en el artículo se estableció de conformidad con lo	

	40 días hábiles, dado que cuando la Gestión de TI es Corporativa, la elaboración del plan de acción requiere de la participación de todas las áreas (Banco y Subsidiarias) involucradas en las acciones que se definan, mismas áreas, que además deben atender su día a día, revisión y análisis de impacto en planes estratégicos, operativos y tácticos, sumado el tiempo de aprobación en los diferentes órganos de dirección (Comité Corporativo Ejecutivo, Comité Corporativo de TI, Juntas Directivas).	establecido en otras normas vigentes aprobadas por el CONASSIF, las cuales, consideran la elaboración de planes de acción.	
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.			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			**Sección IV. Prórrogas**
Artículo 55. Solicitudes de 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.	**[214]BNCR** Se recomienda establecer que la solicitud de prórroga suspende el cómputo del plazo, el cual se reanudará una vez recibida la respuesta de la superintendencia. En igual sentido, se recomienda establecer un plazo para la respuesta por parte del Regulador.	**[214] No procede** Las prórrogas se establecen de conformidad con lo establecido en la ley general de administración pública. El plazo sugerido para el regulador en la observación ya está definido en el artículo 56.	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.
	[215]ABC Los efectos de la solicitud de prórroga deberían operar en forma automática con la gestión presentada antes del vencimiento del plazo, en forma similar a lo que regula la Ley Orgánica	**[215]No procede** Las prórrogas se establecen de conformidad con lo establecido en la ley general de administración pública.	

	de la Procuraduría General de la República. Lo anterior evita que el supervisor tenga que destinar recursos para resolver la gestión (también antes del vencimiento del plazo) y simplifica el trámite, al tiempo que otorga seguridad jurídica.		
	[216]CB Se solicita establecer que la solicitud de prórroga suspende el cómputo del plazo, el cual se reanudará una vez recibida la respuesta de la Superintendencia. En igual sentido, es necesario establecer un plazo para la respuesta por parte del Regulador.	**[216] No procede** Las prórrogas se establecen de conformidad con lo establecido en la ley general de administración pública. El plazo sugerido para el regulador en la observación ya está definido en el artículo 56.	
Las solicitudes de prórroga deben ser presentadas de forma previa al vencimiento del plazo original.			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.			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			**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.			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.			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			**DISPOSICIONES ADICIONALES**
Disposición adicional primera. Referencias normativas			**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			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.			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			**DISPOSICIONES TRANSITORIAS**
Disposición transitoria primera. Auditorías externas de TI			**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.			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.			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			**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.			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			**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.			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			**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:	**[217]BCR** Se solicita considerar que el alcance de la aplicabilidad de este artículo sea solo para contratos que nacen bajo procedimientos de contratación cuando su decisión inicial, se	**[217]No procede** Aplica para todos los contratos. Es necesario que, como parte de los contratos, se consideren las disposiciones incluidas a partir de las presentes modificaciones	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:

	formaliza a partir de la entrada en vigencia de este reglamento.	regulatorias, a fin de contemplar aspectos no incluidos dentro del actual Acuerdo CONASSIF 5-17.	
	[218]ABC La norma transitoria establece el tratamiento de los contratos vigentes, indicando que estos …. Ahora bien, la oración final indica: "dicho plazo no podrá exceder de los doce meses…"; no obstante, la norma transitoria, en la redacción que antecede a lo recién trascrito, no hace mención de ningún plazo, por lo que la referencia resulta inaplicable, lo que requiere ser corregido, considerando, además, la irretroactividad de la norma.	**[218]Procede** Se ajusta la redacción según lo indicado en la observación.	
	[219]ISM Aclarar que este transitorio también aplica para proveedores de servicios de computación en la nube.	**[219]No procede** El transitorio hace referencia en general a contratos vigentes y futuros suscritos con los proveedores de bienes y servicios de TI, por lo que, aplica también a proveedores de servicios de computación en la nube.	
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.			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.	**[220]COOPEFYL** ¿Según considerando b) Se tendría que renegociar todos los contratos a un año?, ¿Qué pasa con las auditorias que están entregando en este momento, los procesos iniciados siguen su curso normal y se terminan? Igual debería indicar si fuera el caso que los contratos tienen posibilidad de prórrogas y que los que nacieron antes de entrada en vigencia de este Reglamento, no le aplique	**[220]No procede** La disposición transitoria primera indica que, 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. Además, se ajustó la redacción de la disposición transitoria para indicar que: ". En todo caso, las entidades y empresas supervisadas	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, las entidades y empresas supervisadas cuentan con un ~~dicho~~ plazo no mayor ~~podrá exceder los~~ a ~~doce~~ dieciocho meses a partir de la entrada en vigor del presente reglamento ~~a fin de que se realicen~~ para realizar los ajustes necesarios en los nuevos contratos y acuerdos de nivel de servicio. En casos debidamente justificados, podrán otorgarse prórrogas de hasta ~~doce~~ seis meses.

	requerimientos no contemplados al inicio de la relación contractual.	cuentan con un plazo no mayor a dieciocho meses a partir de la entrada en vigor del presente reglamento para realizar los ajustes necesarios en los nuevos contratos y acuerdos de nivel de servicio. En casos debidamente justificados, podrán otorgarse prórrogas de hasta seis meses." Por otra parte, es necesario que, como parte de los contratos, se consideren las disposiciones incluidas a partir de las presentes modificaciones regulatorias, a fin de contemplar aspectos no incluidos dentro del actual Acuerdo CONASSIF 5-17.	
	[221]BNCR Para el inciso B, se agradece la aclaración de a qué se refiere el plazo de 12 meses señalado, ya que puede interpretarse que se refiere al plazo de renovación de contratos preexistentes o al plazo de los nuevos contratos. En síntesis, no está claro lo que se está normando para analizar su viabilidad y razonabilidad.	**[221]Procede** Se ajustó la redacción de la disposición transitoria para indicar que: ". En todo caso, las entidades y empresas supervisadas cuentan con un plazo no mayor a dieciocho meses a partir de la entrada en vigor del presente reglamento para realizar los ajustes necesarios en los nuevos contratos y acuerdos de nivel de servicio. En casos debidamente justificados, podrán otorgarse prórrogas de hasta seis meses."	
	[222]CB Se solicita que se aclare a qué se refiere el plazo de 12 meses señalado, ya que puede interpretarse que se refiere al plazo de renovación de contratos preexistentes o al plazo de los nuevos contratos. En síntesis, no está claro lo que se está normando para analizar su viabilidad y razonabilidad.	**[222]Procede** Se ajusta la redacción considerando parte de lo indicado en la observación. Se ajustó la redacción de la disposición transitoria para indicar que: ". En todo caso, las entidades y empresas supervisadas cuentan con un plazo no mayor a dieciocho	

	Adicionalmente, resulta necesario considerar las contrataciones que no vencen en los próximos 12 o 24 meses, cómo establecer los requerimientos contractuales solicitados, y si el proveedor no está de acuerdo y no se puede prescindir del servicio; se debe considerar cómo se tratarán esos casos.	meses a partir de la entrada en vigor del presente reglamento para realizar los ajustes necesarios en los nuevos contratos y acuerdos de nivel de servicio. En casos debidamente justificados, podrán otorgarse prórrogas de hasta seis meses." Por lo tanto, se está otorgando un plazo de dieciocho meses a fin de que la entidad pueda pactar las nuevas condiciones.	
Disposición transitoria quinta. Sociedades corredoras de seguros			**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:			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:			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.			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.			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:			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,			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.			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.			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:			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.			a) La SUGESE podrá requerir a las sociedades corredoras de seguros, la primera auditoría externa de TI a partir de~~l~~ enero del 2027.
Disposición transitoria sexta. Perfil tecnológico			**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.	**[223]COOPEFYL** No se ven estructuras en los lineamientos ni cambios puntuales en el perfil, deberían incluir un anexo adicional con este tema.	**[223]No procede** En la disposición transitoria sexta, se indica que, por el momento, 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. Por lo que, se estarán habilitando espacios para realizar los ajustes y pruebas correspondientes en su debido momento.	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.			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			**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.	**[224]COOPEFYL** Indican que para las brechas debemos de elaborar planes de acción, y que para la implementación de esos planes se tiene un plazo de 3 años a partir de la publicación de este reglamento; pero ¿Cuánto tiempo van a dar para valorar e identificar las brechas?	**[224]Procede** Se ajusta la redacción.	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.
	[225]SAGICOR Disposición transitoria séptima. Párrafo primero y segundo, Favor aclarar en estos párrafos que por planes de implementación se entiende que son para únicamente las brechas de la implementación de COBIT 5.0 a COBIT 2019, para los procesos que cada organización escogió, no significa planes de implementación para la agregación de procesos adicionales.	**[225]No procede** Aplica para todas las brechas que identifique y requiera cerrar la entidad.	
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.	**[226]POPULARVALORES** Con respecto a este transitorio, entendemos que se tienen un plazo máximo de 3 años a partir de la publicación del reglamento para el cierre de brechas; no obstante, no se indica en el transitorio el plazo que estarían dando las Superintendencias para que cada entidad defina el Plan de implementación de brechas que se referencia. En la charla del viernes 26 de abril se indicó que eso depende de cada entidad y la forma en que pretenda atender el tema; sin embargo, en el último párrafo de la disposición sétima se indica que “los planes de implementación deberán estar a disposición de las Superintendencias cuando estas lo requieran”; por lo que consideramos que debe quedar claro el plazo o fecha a partir de la cual las	**[226]Procede** Se ajusta la redacción.	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.

	Superintendencias podrán requerir los planes a las entidades, para lo cual proponemos al menos un año a partir de la publicación del Reglamento. En resumen, se solicita valorar la definición de un plazo para el diseño del Plan de implementación de brechas que no sea menor a un año.		
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:			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 39. Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias
Artículo 40. Comunicado de incidentes a los clientes			Artículo 40. Comunicado de incidentes a los clientes
Artículo 41. Reporte histórico de incidentes			Artículo 41. ~~Reporte~~ Información histórico~~a~~ de incidentes de seguridad de la información y seguridad cibernética
Artículo 45. Comunicación de cambios significativos del perfil tecnológico			Artículo 45. Comunicación de cambios significativos del perfil tecnológico
Artículo 47. Alcance y plazo de la auditoría externa de TI			Artículo 47. Alcance y plazo de la auditoría externa de TI
Artículo 48. Periodicidad de las auditorías externas 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.		Se ajusta la redacción de conformidad con lo indicado en las observaciones 224 y 226, por lo que se define un plazo de dieciocho meses, prorrogable por seis meses.	A partir del sexto mes de la entrada en vigor del reglamento, los planes de implementación para atender brechas 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.”	**[227]BAC** 1. En la organización existen procesos que se ocupan iniciar desde 0. El transitorio 7 brinda la opción de establecer un plan de acción (máximo de 3 años) para ajustarla implementación de este nuevo	**[227]No procede** 1-Los planes de implementación para atender brechas podrán ser considerados para definir los alcances de la auditoría externa de TI o ser considerados como parte de la evaluación de las auditorías	

	reglamento. Sin embargo, la próximo auditoria se ejecutará en ese lapso (3 años). Pero el auditor externo ocupa 1 año de evidencia para poder evaluar el cumplimiento. Consulta. ¿Los procesos que estén matriculados en el plan de implementación, ¿Se pueden excluir de la próxima auditoria? 2.establece un plazo de tres años (no mayor que eso) para elaborar y finalizar los planes de implementación. Por otra parte, debido a su complejidad, periodo de revisión, tipo de negociación y cantidad de servicios, muchos contratos con terceros necesariamente se tendrán que acoger a ese plan de implementación. Sin embargo, este transitorio 7 no está en línea con lo que se indica en el transitorio 4, en donde se establece un período de 12 meses para que todos los contratos vigentes estén modificados de acuerdo con lo que solicita el reglamento. Por los argumentos expuestos anteriormente, consideramos que el transitorio 7 debe contemplar los ajustes en los contratos existentes, ya que no es materialmente posible para la organización renegociar y firmar todos sus contratos con terceros en apenas 1 año.	externas de TI. El supervisor es quien define el alcance de la auditoría externa. 2- Se ajusta la redacción de conformidad con lo indicado en las observaciones 224 y 226, por lo que se define un plazo de dieciocho meses, prorrogable por seis meses.	
	[228]CAMBOLSA Nos queda claro que los regulados cuentan con un plazo de 3 años a partir de la entrada en vigencia de este Reglamento para la ejecutar el Plan de Implementación para cerrar las brechas que se identificaron; no obstante, no queda claro de cuánto tiempo dispondrán para la elaboración de dicho plan, es decir, cuánto tiempo	**[228]No procede** Se ajusta la redacción de conformidad con lo indicado en las observaciones 224 y 226, por lo que se define un plazo de dieciocho meses, prorrogable por seis meses.	

	otorgará el Regulador para la presentación del Plan. Este tema nos preocupa porque el proceso puede ser más complejo para unas entidades que para otras y por lo tanto cada entidad debería poder pactar con el Regulador el plazo de tiempo que considere necesario para la identificación de las brechas y la elaboración del plan. En síntesis, lo que queremos evitar es que el Regulador solicite el Plan de Implementación el un plazo tan corto que algunas entidades no puedan cumplir con esta obligación, de ahí que solicitemos que la Superintendencia evalúe con cada entidad el tiempo mínimo necesario para tener listo dicho Plan.		
	[229]MUCAP Existe una desalineación entre el plazo no mayor de tres años para finalizar los planes de implementación, el cual no está en línea de lo que se indica en el transitorio 4, en donde se establece un período de 12 meses para que todos los contratos vigentes estén modificados de acuerdo a lo que solicita el reglamento., ya que hace que surja la duda si se debe renegociar todos los contratos en 1 año.	**[229] Procede** Se ajusta la redacción de conformidad con lo indicado en las observaciones 224 y 226, por lo que se define un plazo de dieciocho meses, prorrogable por seis meses.	

CONTROL DE CORRESPONDENCIA					
Referencia Sistema de Correspondencia	**Nombre del consultado**	**Alias**	**N° Observaciones**	**Cantidad de Observaciones "Procede"**	**Cantidad de Observaciones "No procede"**
Oficio sin número de referencia	Information Systems Audit and Control Association	ISACA	32	10	22
GG-44-2024	Cooperativa de Ahorro y Crédito de Los Empleados del Sector Público Privado e Independiente	COOPEFYL	30	3	27

Oficio sin número de referencia	Cámara de Bancos e Instituciones Financieras de Costa Rica	CB	29	5	24
GGC-0526-2024	Banco Popular de Desarrollo Comunal	BPDC	16	1	15
Oficio sin número de referencia	Banco Nacional de Costa Rica	BNCR	16	3	13
ABC-0034-2024	Asociación Bancaria Costarricense	ABC	16	5	11
Oficio sin número de referencia	Operadora de Pensiones Complementarias de la Caja Costarricense de Seguro Social	OPC-CCSS	14	3	11
Oficio sin número de referencia	Information & Systems Management	ISM	14	0	14
Oficio sin número de referencia	Banco de Costa Rica	BCR	13	1	12
GO-0243-2024	Bac Credomatic	BAC	9	2	7
Oficio sin número de referencia	Mutual Cartago Ahorro y Préstamo	MUCAP	7	2	5
Oficio sin número de referencia	Quálitas	QUÁLITAS	6	0	6
Oficio sin número de referencia	Coopealianza	COOPEALIANZA	6	1	5
Oficio sin número de referencia	BN Vital OPC	BNVITAL	4	0	4
Oficio sin número de referencia	Aseguradaora Sagicor Costa Rica	SAGICOR	4	0	4
Oficio sin número de referencia	Aseguradora del ISTMO	ISTMO	3	1	2
Oficio sin número de referencia	Popular Pensiones	POPULARPENSIONES	3	1	2
Oficio sin número de referencia	Caja de Ande	CAJAANDE	2	0	2
Oficio sin número de referencia	Vida Plena	VIDAPLENA	2	0	2
Oficio sin número de referencia	Popular Valores	POPULARVALORES	1	1	0
Oficio sin número de referencia	Banco Promerica	PROMERICA	1	0	1
Oficio sin número de referencia	Cámara de Intermediarios Bursátiles y Afines	CAMBOLSA	1	0	1
TOTAL			229	39	190