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-1834/04 y CNS-1835/05, del 27 de noviembre de 2023.

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]BPDC Pregunta** Consulta: Se considerará la ley y reglamento 8968 protección de la persona frente al tratamiento de sus datos personales. ¿Y la Ley 9048 ley delitos informático dentro del código penal?	**[1] 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.	**consideraciones de orden legal y reglamentario**
I. El literal b) del artículo 171 de la Ley Reguladora del Mercado de Valores, Ley 7732, dispone, como una de las funciones del Conassif, aprobar las normas atinentes a la autorización, regulación, supervisión, fiscalización y vigilancia que, conforme a la ley, deben ejecutar la Superintendencia General de Entidades Financieras (Sugef), la Superintendencia General de Valores (Sugeval) y la Superintendencia de Pensiones (Supen). Asimismo, el artículo 28 de la Ley Reguladora del Mercado de Seguros, Ley 8653, dispone, en relación con la Superintendencia General de Seguros (Sugese), que: "al superintendente y al intendente les serán aplicables las disposiciones establecidas, de manera genérica y de			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

aplicación uniforme, para las demás Superintendencias bajo la dirección del Conassif y sus respectivos superintendentes e intendentes".			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, 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.			IV. El artículo 3 de la Ley Reguladora del Mercado de Valores, Ley 7732, establece que la Sugeval debe velar por la protección del inversionista y la transparencia del mercado de valores. Asimismo, el artículo 8 de la Ley 7732, inciso b), establece que la Sugeval someterá a la consideración del Consejo Nacional los proyectos de reglamento que le corresponda dictar a la Superintendencia. El inciso j) establece la potestad de adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación, supervisión y fiscalización que le competen, y el inciso l) establece la potestad de la Superintendencia para requerir a los supervisados toda la información razonablemente necesaria a fin de cumplir la función supervisora del mercado de valores.
V. El artículo 38, literal f) del Régimen Privado de Pensiones, Ley 7523, establece como una atribución del superintendente de Pensiones adoptar todas las acciones necesarias para el cumplimiento efectivo de			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.			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 de riesgos, entre otros, para cumplir la supervisión que debe realizar cada una de las Superintendencias.			VII. El inciso n) y el sub inciso xi) del artículo 131 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558; el inciso r) del el artículo 38 de la Ley de Régimen Privado de Pensiones, Ley 7523; el inciso L) del artículo 8 de la Ley Reguladora del Mercado de Valores, y los incisos i) y j) del artículo 29 de la Ley Reguladora del Mercado de Valores, Ley 8653, facultan por su orden a la Superintendencia General de Entidades Financieras, a la Superintendencia de Pensiones, a la Superintendencia General de Valores y a la Superintendencia General de Seguros, a proponer al Conassif normas sobre el contenido, la forma y la periodicidad con que las entidades deben proporcionar a la Superintendencia, información sobre su situación jurídica, económica, financiera, de gobierno corporativo y de administración de riesgos, entre otros, para cumplir la supervisión que debe realizar cada una de las Superintendencias.
VIII. El inciso e) del artículo 131 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558; el artículo 40 de la Ley de Régimen Privado de Pensiones, Ley 7523; el inciso j) del artículo 8 de la			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

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.			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:	**[2]COOPEFYL** De conformidad con el Acuerdo Sugef 25-23, la Coopefyl se encuentra dentro de la regulación	**[2] No procede** Conviene aclarar que el Acuerdo SUGEF 25-23 establece en su artículo 5 que, las disposiciones sobre gobierno	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:

	proporcional emitida por ese Ente que entró en vigencia el pasado 10 de julio del 2023, donde se le exime de la regulación de Gobierno Corporativo, Idoneidad y Gestión de Riesgos. Por lo tanto, la presente normativa debe ser consistente en el tema del Marco de Gobierno y de Gestión de TI de una regulación simplificada según el nivel de riesgo de las cooperativas sujetas a la proporcionalidad establecida por la misma SUGEF, reiterando por parte de la Coopefyl que no buscamos que se nos exima de temas tan relevantes , sino que se aplique una simplificación regulatoria según el nivel de riesgo de la entidad, situación diferente a lo establecido por SUGEF en el Acuerdo 25-23 y contraria a los principios de BASILEA III que reforzó sus estándares para que la regulación y supervisión se ejecutara basada en Riesgos(SBR) y proporcional a los riesgos de los regulados, pero no eliminando su aplicación. En los Capítulos IV y V no se establece la proporcionalidad y en los lineamientos tampoco se define. La regulación del marco de gobierno y de gestión de TI debe ser proporcional a los riesgos y la naturaleza de la entidad regulada. Las cooperativas de ahorro y crédito en el ámbito de la proporcionalidad según lo definido en el Acuerdo Sugef 25-23, están expuestas a riesgos	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. Con relación a los riesgos tecnológicos, de seguridad fraudes y fallas en la gestión de los datos ya existen leyes específicas relacionadas con la protección de la persona frente al tratamiento de datos personales ley 8968 y para los fraudes en la ley 9048. Los riesgos tecnológicos, los riesgos de seguridad de la información y los riesgos de seguridad cibernética deben ser atendidos por las entidades supervisoras de conformidad con lo dispuesto en la presente propuesta regulatoria de manera proporcional considerando el tamaño, complejidad y modelo de negocio. En todo caso las entidades como requerimiento regulatorio y como mejor práctica deberán implementar procesos integrales de gestión de riesgos que permitan dar un tratamiento apropiado a cada riesgo de conformidad con su apetito y tolerancia al riesgo.	

	específicos relacionados con la tecnología, incluidos riesgos de seguridad cibernética, fraudes y fallas en la gestión de datos. Por lo tanto, independientemente de las exenciones en otras áreas, es prudente definir regulaciones específicas de TI para mitigar estos riesgos. Cualquier regulación debe ser proporcional a los riesgos y la naturaleza de la entidad regulada. Para las cooperativas del Acuerdo SUGEF 25-23, las regulaciones demasiado onerosas podrían no ser viables o necesarias.		
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.	**[3]Luis Diego León Barquero** En el inciso a del punto XII, se habla de órganos de Dirección, pero para mí serían órganos de gobierno, y pondría Junta Directiva o equivalente, así como los comités de la Junta Directiva o equivalente. En el inciso a del punto XII, se habla de Alta Gerencia, pero para mí serían Alta administración. En el inciso a del punto XII, se habla de órganos de control, pero no entiendo a qué se refiere con este término y el por qué está separado del gobierno y la administración.	**[3] No procede** La propuesta reglamentaria incorpora como propias las definiciones utilizadas en las demás reglamentaciones vigentes aprobadas por el CONASSIF, como es el caso del Reglamento de Gobierno Corporativo, Acuerdo Conassif 4-16.	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.
	[4]ISACA Considero importante también considerar las funciones de los Órganos de Dirección y Control sobre las responsabilidades dentro del marco de Gobierno y Gestión de TI en relación con la tercerización de Bienes y	**[4] No procede** Con relación a los pilares y su integración: a-Dentro de la sección de “considerandos” de la presente modificación reglamentaria, se incluye los considerandos denominados “otras consideraciones”, donde se aclara que la	

	Servicios de TI, la Computación en la Nube sobre todo desde la perspectiva de Protección y Privacidad de los datos, en su tratamiento de uso y acceso, como se menciona en el inciso b (siguiente). Considero que, en la modificación integral mencionada, se debe conectar de forma explícita varios pilares en la arquitectura empresarial, a saber: Gestión de Riesgos, Continuidad del Negocio y Gestión de Seguridad de la Información (ya considerado). Un segundo aspecto relevante en la modificación integral es la relevancia de procesos como Gestión de Proyectos, Desempeño y Capacidad y contratación (ya considerado) de servicios y productos I&T.	propuesta de modificación reglamentaria está alineada 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. Con relación a los procesos relevantes y los servicios y productos de I&T: a-Según lo indicado en el Artículo 43 Procesos de evaluación del marco de gobierno y gestión, las entidades y empresas supervisadas deben realizar un estudio técnico para valorar la relevancia de sus procesos y evaluar cuáles procesos no les aplican de conformidad con el principio de proporcionalidad, tamaño, complejidad y modelo de negocio. b-Tratándose de marcos de referencia diseñados por la industria de tecnología, en el caso de CobiT 2019 el término I&T hace referencia a la Información y a las Tecnologías, y el Término TI, hace referencia al área de TI. c-En la propuesta reglamentaria desde las versiones previas del reglamento se utiliza el término unidad y gestión de TI para hacer referencia al área de TI y se utiliza el término TI, el cual, contempla el concepto del marco de referencia y lo amplía de la siguiente forma: 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.	
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 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.	**[5]BPDC Pregunta** ¿Se considerará la protección y privacidad de datos según la Ley y Reglamento 8968?	**[5]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.	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.
	[6]BCR En relación con el punto "a" aclarar si se está viendo de forma separada la gestión de la seguridad de la información de la gestión de la seguridad cibernética.	**[6] No procede** La norma ISO 27032 revela que la seguridad cibernética es un subdominio de la seguridad de la información. Adicionalmente, las entidades y empresas supervisadas para su modelo de negocio deben establecer los elementos de control del modelo de líneas defensa, considerando entre otras el principio de proporcionalidad, su tamaño y complejidad, razón por la cual, la propuesta reglamentaria incorpora en el "Artículo 32 Seguridad cibernética" lo siguiente: Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital. Las entidades y empresas supervisadas deben establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética.	
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 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.	**[7]COOPEFYL** Coopefyl reitera que el gobierno de TI no es un elemento aislado dentro de una organización, sino que es una parte esencial del gobierno corporativo. El gobierno corporativo abarca las reglas, prácticas y procesos a través de los cuales se dirige y controla una empresa. La inclusión del gobierno de TI dentro del gobierno corporativo refleja el reconocimiento de que la tecnología de información es crítica para el éxito y la sostenibilidad de una organización moderna. No obstante , la SUGEF debe definir una alineación según lo definido en el Acuerdo Sugef 25-23 y los temas de tecnología de información que plantea el presente reglamento, en razón de que vayan en la misma dirección de implicación regulatoria según el nivel de riesgo de la entidad, no buscando su eliminación como acordó la SUGEF en el Acuerdo 25-23 referidos a otros temas, contrario a los principios de BASILEA III, que reforzo sus estándares para que la regulación y supervisión se ejecutara basada en Riesgos (SBR). Se debe asegurar el ente regulador que lo establecido en los capítulos IV, V y en los lineamientos generales cumplan el tema de la proporcionalidad. Coopefyl R.L. atiende lo establecido en el Acuerdo Sugef 25-23 sobre proporcionalidad. La SUGEF	**[7] 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. Con relación a los riesgos tecnológicos, de seguridad fraudes y fallas en la gestión de los datos. Ya existen leyes específicas relacionada con la protección de la persona frente al tratamiento de datos personales ley 8968 y para los fraudes en la ley 9048. Los riesgos tecnológicos, los riesgos de seguridad de la información y los riesgos de seguridad cibernética deben ser atendidos por las entidades supervisoras de conformidad con lo dispuesta en la presente propuesta regulatoria de manera proporcional considerando el tamaño, complejidad y modelo de negocio. En todo caso las entidades como requerimiento regulatorio y como mejor práctica deberán implementar procesos integrales de gestión de riesgos que permitan dar un tratamiento apropiado a cada riesgo de conformidad con su apetito y tolerancia al riesgo.	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.

	estableció eximir del gobierno corporativo, idoneidad y competencias a las cooperativas de ahorro y crédito menores a ochenta mil millones de colones, aún cuando BASILEA III, establece que la proporcionalidad debe simplificarse según el nivel de riesgo y no eximirse como se indica en el Acuerdo 25-23. No obstante lo anterior, el Consejo de Administración de la COOPEFYL reitera su papel activo y estratégico en la gobernanza de TI, asegurando que la tecnología esté alineada con los objetivos de la cooperativa, gestionada con seguridad y eficiencia, y utilizada de manera que beneficie a sus miembros y fortalezca la posición de la cooperativa en el mercado.		
	[8]FEDEAC Pregunta XIII: ¿Debemos interpretar que la dependencia de las funciones operativas de Gobierno de TI y Control Interno de TI debería tener dependencia administrativa de Gobierno Corporativo o directamente del Órgano de Dirección como los demás órganos de control?	**[8] No procede** Se incluye en la sección de preguntas y respuestas Respuesta: a. El reglamento de Gobierno Corporativo del CONASSIF, en el "Artículo 3 Definiciones" indica que: el Gobierno Corporativo es un conjunto de relaciones entre la administración de la entidad, su Órgano de Dirección, sus propietarios y otras Partes Interesadas, las cuales proveen la estructura para establecer los objetivos de la entidad, la forma y los medios para alcanzarlos y monitorear su cumplimiento. El Gobierno Corporativo define la manera en que se asigna la autoridad y se toman las decisiones corporativas. b. En los "Considerados" de la propuesta del reglamento en el título	

		"Consideraciones sobre el gobierno de la tecnología de información" indica entre otros aspectos que el gobierno de la tecnología de información es un subdominio 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.	
	[9]ISACA Se indica que el marco de gobierno y de gestión de TI puede ser compartido a nivel corporativo, pero si no se hace así, ya que está la opción, se debería activar el nivel de gobierno empresarial, es decir, varios distintos gobiernos empresariales de un Grupo Financiero, puede convertirse en Gobierno Corporativo o implementarlo a ese nivel por empresa. No sólo lo limitaría a "seguridad de la información" yo haría referencia a los mismos riesgos y objetivos discutidos en el numeral b, como parte de esa mejora deseada: "gobierno y gestión sobre los riesgos comunes y emergentes, que afectan la seguridad de la información, la seguridad cibernética, pudiendo materializar incidentes relacionados, producto de la tercerización de bienes y servicios de TI así como su cadena de suministro, computación en la nube, así como el tratamiento de uso y acceso a los datos y activos de información en general". En resumen, se trata de garantizar un	**[9] No procede** Se atiende como parte de la observación [8] Adicionalmente, con relación a los temas de los riesgos el artículo 1 Objeto indica entre otros aspectos, pero no limitado lo siguiente: 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. El marco de gobierno y gestión de TI incluye procesos relacionados a la administración de riesgos de TI. Las entidades y empresas supervisadas deben establecer si la gestión de riesgos se hace a nivel empresarial o se implementa solo a nivel de TI, lo anterior de conformidad con el modelo de negocio, tamaño y complejidad. En todo caso, dichos procesos deben valorar los riesgos asociados con seguridad cibernética, presentes en la gestión de terceros y la cadena de suministros, computación en la nube, así como en el uso y acceso a los datos.	

	gobierno y la gestión de los riesgos de seguridad de la información, seguridad cibernética, presentes en la gestión de terceros y la cadena de suministros, computación en la nube, así como en el uso y acceso a los datos.		
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.	**[10]Luis Diego León Barquero** Buenas Prácticas de Gobierno Corporativo. El texto parece indicar que la Junta Directiva y la Alta Administración tienen las mismas responsabilidades y funciones.	**[10] No procede** El Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, tiene como objeto establecer los principios sobre Gobierno Corporativo que deben considerar las entidades incluidas en el alcance de dicho Reglamento, brindado una serie de estándares cualitativos que reflejan fielmente las sanas prácticas internacionales, cuya aplicación depende de los atributos particulares de cada entidad y deben ser aplicados respetando, en todo momento, el ordenamiento jurídico que rige para el Sistema Financiero Nacional. Las responsabilidades y funciones particulares de los Órganos de Dirección y de la Alta Gerencia en temas de tecnologías de información, seguridad de la información y ciberseguridad, por su naturaleza y especialización se establecerán en el Reglamento General de Gobierno y gestión de TI.	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.

	[11]COOPEANDE Es importante considerar cuando se indica que los Órganos de Dirección y de la Alta Gerencia se vean comprometidos a adaptar e implementar sus mediadas de gobierno conforme a su contexto, necesidades específicas y riesgos, no dejas de lado que las principales prácticas se basan en la estratégica particular de cada organización, por ende, el adaptar e implementar el gobierno debe estar alineado a la estrategia organizacional.	**[11] No procede** El diseño, implementación, monitoreo y mejora de los marcos de control interno en las entidades y empresas supervisadas debe ser guiado por la adopción y adaptación de estándares, marcos de referencias, y buenas prácticas internaciones a fin de atender el marco regulatorio vigente. La adopción y adaptación debe estar en función de los objetivos de la organización, a fin de lograr una optimización de los recursos, los riesgos, y maximizar los beneficios. Un factor crítico de éxito para la adopción y adaptación es el compromiso del Órgano de Dirección y la Alta Gerencia para adaptar e implementar los controles conforme a su contexto, necesidades específicas, riesgos y las particularidades de cada entidad o empresa supervisada.	
	[12]FEDEAC XIV: Es importante considerar cuando se indica que los Órganos de Dirección y de la Alta Gerencia se vean comprometidos a adaptar e implementar sus mediadas de gobierno conforme a su contexto, necesidades específicas y riesgos, no deja de lado que las principales prácticas se basan en la estratégica particular de cada organización, por ende, el adaptar e implementar el gobierno debe estar alineado a la estrategia organizacional.	**[12] No procede** El diseño, implementación, monitoreo y mejora de los marcos de control interno en las entidades y empresas supervisadas debe ser guiado por la adopción y adaptación de estándares, marcos de referencias, y buenas prácticas internaciones a fin de atender el marco regulatorio vigente. La adopción y adaptación debe estar en función de los objetivos de la organización, a fin de lograr una optimización de los recursos, los riesgos, y maximizar los beneficios. Un factor crítico de éxito para la adopción y adaptación es el compromiso del Órgano de Dirección y la Alta Gerencia para adaptar e implementar los controles conforme a su contexto,	

		necesidades específicas, riesgos y las particularidades de cada entidad o empresa supervisada.	
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 cibernética.	**[13]COOPEFYL** De conformidad con el Acuerdo Sugef 25-23, la Coopefyl se encuentra dentro de la regulación proporcional emitida por ese Ente que entró en vigencia el pasado 10 de julio del 2023, donde se le exime de la regulación de Gobierno Corporativo, Idoneidad y Gestión de Riesgos. Por lo tanto, la presente normativa debe ser consistente en que el tema de Gobierno y de Gestión de TI, vaya en la misma dirección de simplificación regulatoria según el nivel de riesgo de la entidad, no buscando su eliminación como acordó la SUGEF en el Acuerdo 25-23, contrario a los principios de BASILEA III, que reforzó sus estándares para que la regulación y supervisión se ejecutara basada en Riesgos (SBR). En los Capítulos IV y V no se establece la proporcionalidad y en los lineamientos en el ANEXO #2 "Procesos de evaluación del marco de Gestión de TI para la regulación Proporcional" se establecen una serie de procesos para evaluar el marco de Gestión de TI y en el artículo 3 del presente reglamento se exime de la aplicación del Marco de Gobierno y de Gestión de TI a las cooperativas sujetas de	**[13] 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. Con relación a los riesgos tecnológicos, de seguridad fraudes y fallas en la gestión de los datos. Ya existen leyes específicas Adicionalmente, se modifica el texto para mayor claridad.	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.

	la regulación Proporcional, con lo cual, existe una gran contradicción. Además, que no hay una descripción del alcance de esos procesos como si se incluye en el ANEXO 1 para los otros entes regulados.		
	[14]BCR 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.	**[14]No procede** 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.	
	[15]ISACA El título dice mucho, y el contenido solo se enfoca en TI y en la seguridad cibernética, dejando de lado la continuidad de las operaciones del negocio.	**[15]No procede** Se aclara que el contenido del considerando incluye procesos de negocio y servicios de TI resilientes que minimicen el impacto de las amenazas.	
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 empresas	**[16]ISACA** Debería haber una relación explícita entre la gestión de riesgos y su relación con el gobierno de TI y el empresarial.	**[16]No procede** La propuesta de modificación reglamentaria en el "Artículo 1. Objeto", 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	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.		Gobierno Corporativo, Acuerdo CONASSIF 4-16 y en el marco de regulación vigente sobre gestión de riesgos de cada Superintendencia. De forma adicional, en el "Capítulo II Gobierno y Gestión de TI" se establecen responsabilidades especificas con relación al Órgano de Dirección, Alta Gerencia, y Órganos o funciones de control en la organización entre las que se detallan la Auditoría Interna y la gestión de riesgos.	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.	**[17]COOPEFYL** Coopefyl R.L. atiende lo establecido en el Acuerdo Sugef 25-23 sobre proporcionalidad. La SUGEF estableció eximir del gobierno corporativo, idoneidad y competencias a las cooperativas de ahorro y crédito menores a ochenta mil millones de colones, aún cuando BASILEA III, establece que la proporcionalidad debe simplificarse según el nivel de riesgo y no eximirse como se indica en el Acuerdo 25-23. Es necesario que la SUGEF detalle los alcances del anexo 2 en los lineamientos generales, "regulación Proporcional" sobre los procesos de gestión de TI que deben ser evaluados por la Auditoría Externa ya que no se incluye ninguna descripción o alcance como si se establece en el Anexo 1 para los otros regulados. Además, no se observa ninguna diferenciación de proporcionalidad en los artículos de los capítulos IV y V, para las cooperativas de ahorro y crédito	**[17] 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. Los riesgos tecnológicos, los riesgos de seguridad de la información y los riesgos de seguridad cibernética deben ser atendidos por las entidades supervisoras de conformidad con lo dispuesta en la presente propuesta regulatoria de manera proporcional considerando el tamaño, complejidad y modelo de negocio. En todo caso las entidades como requerimiento regulatorio y como mejor práctica deberán implementar procesos integrales de gestión de riesgos que permitan dar un tratamiento apropiado a cada riesgo de conformidad con su apetito y tolerancia al riesgo. Adicionalmente, se aclara que:	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.

	del Acuerdo SUGEF 25-23. Coopefyl R.L. atiende lo establecido en el Acuerdo Sugef 25-23 sobre proporcionalidad. La SUGEF estableció eximir del gobierno corporativo, idoneidad y competencias a las cooperativas de ahorro y crédito menores a ochenta mil millones de colones, aún cuando BASILEA III, establece que la proporcionalidad debe simplificarse según el nivel de riesgo y no eximirse como se indica en el Acuerdo 25-23. Es conveniente que la SUGEF establezca la proporcionalidad el marco de gestión de TI para las cooperativas de ahorro y crédito sujetas a la normativa SUGEF 25-23, ya que el Anexo 2 de los Lineamientos Generales sólo se mencionan los procesos de gestión de TI que deben ser evaluados por la Auditoría Externa sin conocer ningún alcance o descripción de los mismos.	El reglamento General de Gobierno y Gestión de TI, en el "Artículo 47. Alcance y plazo de la auditoría externa de TI", se establece entre otros aspectos que: "[…]Las Superintendencias deben comunicar a las entidades y empresas supervisadas, el alcance de la auditoría externa de TI". Por otra parte, la aplicación proporcional y diferenciada del Reglamento General de Gobierno y Gestión de TI establece que los procesos del Marco de Gestión de TI para las entidades supervisadas por SUGEF sujetas a la Regulación proporcional para cooperativas de ahorro y crédito, Acuerdo SUGEF 25-23 son 13 y para las sociedades corredoras de seguros supervisadas por SUGESE son 9, dichos procesos están en el Anexo 2 de los lineamientos que acompañan el reglamento.	
	[18]COOPEANDE Con respecto a que el marco de gestión de TI requiere de esfuerzo planificado y progresivo. Además, requiere se considere el entendimiento de la estrategia y su contexto organizacional, la determinación del alcance y la aplicación de los componentes a implementar. Es importante que se puede dejar más claro que cada entidad debe definir el alcance de implementación del Marco de Gobierno y Gestión de TI con base	**[18] No procede** El reglamento General de Gobierno y Gestión de TI, en los considerandos indica entre otros que: i El diseño e implementación del marco de gestión de TI requiere de esfuerzo planificado y progresivo. ii. 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	

	en su estrategia, contexto y sus riesgos.	dependencia tecnológica de sus actividades. Po otra parte, las entidades al tomar como referencia para la implementación, por ejemplo, un marco de referencia, tal como es el caso de CobiT 2019, este marco indica que los factores de diseño son factores que pueden influir en el alcance del diseño del sistema de gobierno de una entidad o empresa supervisada y posicionarla para que tenga éxito al usar TI, entre los que están: 1. Estrategia empresarial 2. Metas empresariales 3. Perfil de riesgo 4. Problemas relacionados con TI 5. Panorama de amenazas 6. Requerimientos de cumplimiento 7. Rol de TI 8. Modelo de abastecimiento para TI 9. Métodos de implementación de TI 10. Estrategia de adopción de tecnología 11. Tamaño de la empresa 12. Factores futuros Finalmente, los lineamientos que acompañan al Reglamento General de Gobierno y Gestión de TI, en el título "Aspectos por considerar para la elaboración del estudio técnico que fundamenta los procesos de evaluación del marco de gobierno y gestión de TI no aplicables", incluyen que los criterios para la evaluación de la aplicabilidad de los procesos consideren, al menos: 1. Cascada de metas adaptada a la entidad o empresa supervisada 2. Factores de diseño adaptados a la entidad o empresa supervisada 3. Consideraciones de la naturaleza, tamaño, volumen de operaciones,	

		modelo de negocio y riesgos de la entidad o empresa supervisada.	
	[19]FEDEAC XVII: Es importante que se deje más claro que cada entidad debe definir el alcance de implementación del Marco de Gobierno y Gestión de TI con base en su estrategia, contexto y sus riesgos.	**[19]No procede** Ver respuesta de la observación 18.	
	[20]COOPEBANPO Sobre este aspecto, consideramos que el marco de gestión debe seguir siendo definido a través de un análisis interno (o externo por parte de la auditoria) de acuerdo con las condiciones propias de cada entidad y atendiendo los criterios que la superintendencia a definido, tales como apetito al riesgo, volumen de negocio, naturaleza de las operaciones, etc.	**[20]No procede** Ver respuesta de la observación 18.	
	[21]CCPA Consideramos importante que se incluyan medidas para mitigar los riesgos, utilizando el modelo COBIT 2019 de referencia; una de las situaciones que los contadores públicos autorizados encuentran en las instituciones reguladas es que el modelo de riesgos no contempla los riesgos de TI.	**[21] No procede** La propuesta del Reglamento General de Gobierno y Gestión de TI incluye en el "Artículo 15", las responsabilidades de la unidad o función de gestión de riesgos relacionadas con las tecnologías de información, la unidad o función de gestión de riesgos. Por otra parte, la propuesta de modificación regulatoria está plenamente integrada y complementaria al marco de regulación vigente sobre gestión de riesgos de cada Superintendencia.	
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	**[22]OPC-CCSS**	**[22] Procede**	XVIII. La migración a la nube brinda enormes oportunidades, eficiencias y conveniencia, sin embargo,

embargo, también expone a las organizaciones a una nueva gama de amenazas de seguridad cibernética.	Es necesario que se aclare que la consideración XVIII corresponde al modelo de nube híbrida o nube pública, dado que existen modelos de nube dentro de los cuales está el modelo de nube privada y en este no necesariamente se tiene un modelo de responsabilidad compartida con algún proveedor ya que la entidad lo puede controlar en un 100% a nivel administrativo y técnico.	Se incorpora parte de lo sugerido para mejorar la redacción del texto.	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 el modelo de responsabilidades compartidas entre el cliente (gestión propia) y el proveedor (tercerización) aplicables para cada uno de los modelos de servicios de computación en la nube, así como los controles administrativos y técnicos asociados a este tipo de servicios.	**[23]Luis Diego León Barquero** No creo que un marco de gobierno y gestión incluya medidas sólidas para mitigar los riesgos, pues esto forma parte de la Administración de Riesgos y el objetivo de COBIT 2019 de administración de riesgos. El problema que yo he encontrado en varias entidades es que el modelo de administración de riesgos no contempla en algunos casos los riesgos de TI.	**[23] No procede** La propuesta del Reglamento General de Gobierno y Gestión de TI incluye en el "Artículo 15", las responsabilidades de la unidad o función de gestión de riesgos relacionadas con las tecnologías de información, la unidad o función de gestión de riesgos. Por otra parte, la propuesta de modificación regulatoria está plenamente integrada y complementaria al marco de regulación vigente sobre gestión de riesgos de cada Superintendencia.	XIX. Es importante que las entidades y empresas supervisadas tengan definidaso ~~el modelo de responsabilidades compartidas entre el cliente (gestión propia) y el proveedor (tercerización)~~ 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.
	[24]BNCR ¿Existe un plazo de implementación para abordar todos los ajustes que se están proponiendo en este nuevo acuerdo?	**[24] 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.	
	[25]BPDC Entendemos que el modelo es propio de la organización, pero al final lo válido es lo definido en el contrato con el tercero	**[25] Procede** Se ajusta la redacción para aclarar el texto.	
	[26]COOPEBANPO Es correcta esta apreciación, no obstante, no se puede dejar de lado la criticidad de los servicios que se	**[26] Procede** Se ajusta la redacción para aclarar el texto.	

	tienen en la nube o tercerizados. No solo por el hecho de estar en una nube significa que son servicios que deberían cumplir con todos los requerimientos de ciberseguridad, a lo mejor son servicios no críticos que se pueden mantener en nube y sobre los cuales la entidad no asume mayor riesgo.		
	[27]BCR Detallar cuál es el contenido mínimo que se debe considerar, para el modelo de responsabilidades compartidas, así como en los controles administrativos y técnicos.	**[27] No procede** Se modificó la redacción. Ya no se indica "modelo de responsabilidades compartidas".	
consideraciones prudenciales sobre la tercerización de bienes y servicios de TI			
XX. Los proveedores de bienes y servicios son ampliamente utilizados para proporcionar servicios, sistemas y soluciones de TI que respaldan las operaciones de las organizaciones. Las vulnerabilidades de seguridad cibernética producto de la tercerización de bienes y servicios de TI podrían convertirse en canales de ciberataques, por lo que las capacidades de seguridad cibernética de los proveedores son elementos críticos.	**[28]ISACA** El impacto de la tercerización está en todos los alcances de la seguridad, no solo en la cibernética. Se ocupa algo más que solo acuerdos escritos, se deben establecer los controles preventivos del suministro de elementos o componentes críticos y sensibles. Estos controles deben ser parte de los lineamientos generales, ya que deberán conformar la plantilla contractual sugerida y minimizar la probabilidad de contratos que esté firmados y contengan vicios con respecto al cumplimiento normativo. Lo anterior se incrementa cuando se cuenta con contratos de adhesión, lo más común en	**[28] Procede** Se ajusta la redacción del texto. El Reglamento General de Gobierno y Gestión establece las expectativas de alto nivel que las superintendencias esperan que las entidades y empresas supervisadas implementen con el fin de contribuir en un ambiente de control interno efectivo en sus organizaciones. b. Entre dichas expectativas y en particular para atender los riesgos de externalización, están al menos, las disposiciones establecidas en la "Sección IV Tercerización de bienes y servicios de TI", y en los "Artículo 6. Marco de Gobierno y Gestión de TI" y el "Artículo 7. Propósitos del marco de gobierno y gestión de TI". c. Adicionalmente, con relación al diseño e implementación de los controles preventivos, detectivos, o correctivos, el Reglamento incluye en	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.

	servicios públicos, si un proveedor de nube no cumple con algunos términos de cumplimiento normativo indicados en la norma no podría renovar su contrato o del todo no puede participar en las licitaciones públicas o privadas de las entidades o empresas supervisadas.	sus lineamientos que las entidades y empresas supervisadas pueden utilizar (adoptar y adaptar) 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. d. El marco de control interno de la organización en todo momento debe responder a su estratégica, lo anterior, con el fin de mitigar los riesgos, y considerando el principio de proporcionalidad, el cual contempla entre otros, pero no limitado aspectos tales como: el tamaño, complejidad y modelo del negocio.	
XXI. Los proveedores de bienes y servicios de TI y su cadena de suministros no están dentro del alcance de esta regulación, sin embargo, es necesario que las entidades y empresas supervisadas asuman su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados; lo anterior, a través de cláusulas en los contratos y acuerdos de servicio que soliciten la inclusión de las prácticas y controles para mitigar los riesgos de tercerización de bienes y servicios de TI.	**[29]Luis Diego León Barquero** En el punto XXI, indica "lo anterior, a través de cláusulas en los contratos y acuerdos de servicio que soliciten la inclusión de las prácticas y controles para mitigar los riesgos de tercerización de bienes y servicios de TI." Yo cambiaría la redacción a este punto: "lo anterior, por ejemplo, a través de cláusulas en los contratos y acuerdos de servicio que soliciten la inclusión de las prácticas y controles para mitigar los riesgos de tercerización de bienes y servicios de TI". Sería conveniente establecer que informes de aseguramiento de auditores para los servicios de los proveedores, como los informes de auditoría en la ISO27001 Gestión de la Seguridad de la	**[29] Procede** Se ajusta la redacción considerando parte de la observación.	XXI. Los proveedores de bienes y servicios de TI y su cadena de suministros no están dentro del alcance de esta regulación, sin embargo, es necesario que las entidades y empresas supervisadas asuman su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados; lo anterior, a través de 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.

	Información u otros informes de aseguramiento basados en la Norma Internacional de Encargos de Aseguramiento3402 Informes de aseguramiento sobre los controles en las organizaciones de servicios.		
	[30]BPDC 1-En el apartado XXI, nos preocupa que si bien se menciona que estos proveedores y su cadena de suministros no están en el alcance y que cada uno tendrá que asumir esa responsabilidad, si sería recomendable analizar incluir el tema ya que podría dejar ciertos aspectos de ciberseguridad sin una supervisión o gestión adecuada Se propone el siguiente texto: "Los proveedores de bienes y servicios de TI deberán atender los requisitos de las entidades y empresas supervisadas según su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados; lo anterior, a través de cláusulas en los contratos y acuerdos de servicio que soliciten la inclusión de las prácticas y controles para mitigar los riesgos de tercerización de bienes y servicios de TI Por otra parte, entendemos que será una responsabilidad del Banco determinar cuáles cláusulas definir y que acceso a sus	**[30] No Procede** La regulación no puede establecer disposiciones a los proveedores de bienes y servicios de TI porque no son regulados. 2-El considerando no se enfoca en lo indicado. Sin embargo, en diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión.	

	lineamientos en Seguridad y otros deberá asegurarle al Proveedor. En el apartado XXII, entendemos que generalmente una empresa no tiene el suficiente músculo para pedir condiciones diferenciadas a proveedores como Amazon. Por eso aplica el contrato de adhesión (aceptar las condiciones del proveedor). 2-CONSULTA: ¿Cómo la Entidad Supervisada gestionará ante el Regulador la aplicación de excepciones producto del uso de instrumentos de adhesión?		
	[31]OPC-CCSS Sobre la consideración XXI: Si bien es cierto que en un contrato de servicios se genera un contrato y eventualmente un acuerdo de nivel de servicio, no es cierto que en la adquisición de bienes el comportamiento sea idéntico y por ende, resulta complejo por ejemplo exigir un acuerdo de servicio para la estricta compra de bienes de TI. Lo que sí puede hacer la entidad regulada es disponer de una serie de prácticas y controles para mitigar riesgos ante el uso y adquisición de bienes pero nunca podrán ser asociados a un acuerdo de servicio ante la compra de bienes.	**[31] No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión. Tal como se indica en el considerando, las entidades y empresas supervisadas deben asumir su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados, lo anterior se logra a través de mecanismos de control, tales como cláusulas 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, o aceptación de términos y condiciones de la organización por parte de terceros, o auditorías externas, entre otros.	
	[32]CCPA El Colegio de Contadores Públicos de Costa Rica considera de importancia que las entidades reguladas soliciten a los	**[32]No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión.	

	proveedores de servicios informes de aseguramiento sobre los aspectos regulatorios, los cuales no forman parte de una opinión de estados financieros.	La propuesta reglamentaria establece que las entidades deberán contratar auditorías externas de TI, las cuales, deberán ser realizadas 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 cuenten con auditorías independientes.	
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 cibernética, sin embargo, sus servicios suelen contratarse mediante instrumentos de adhesión; lo que hace necesario establecer un tratamiento diferenciado en la aplicación de la regulación, de manera que el marco regulatorio no impida la contratación de servicios con esos proveedores ni la supervisión por parte de las Superintendencias. En los casos en que los servicios se contraten mediante instrumentos de adhesión, la entidad debe ser responsable de asegurar la confidencialidad y la continuidad de los bienes y servicios delegados.	**[33]BNCR Pregunta** ¿Los acuerdo a nivel de servicio pueden estar dentro del contrato o deben ser independientes (contrato y acuerdo)?	**[33]No procede** Se incluye la respuesta en la sección de preguntas frecuentes que se publicará en el sitio web de cada Superintendencia.	XXII. Los más reconocidos proveedores internacionales de servicios en la nube, servicios de cómputo, almacenamiento, bases de datos, análisis e inteligencia artificial se encuentran a la vanguardia en el uso de herramientas e implementación de políticas de seguridad de la información y seguridad cibernética, sin embargo, sus servicios suelen contratarse mediante instrumentos de adhesión; lo que hace necesario establecer un tratamiento diferenciado en la aplicación de la regulación, de manera que el marco regulatorio no impida la contratación de servicios con esos proveedores ni la supervisión por parte de las Superintendencias. En los casos en que los servicios se contraten mediante instrumentos de adhesión, la entidad debe ser responsable de asegurar la confidencialidad y la continuidad de los bienes y servicios delegados.
	[34]COOPEANDE Se debe considerar que los contratos de adhesión de servicios nube, computo, almacenamiento, etc. Son muy estándar y es complejo realizar ajustes sobre los mismos, casi que las organizaciones que requieren de estos servicios deben aceptar los contratos tal cual están definidos por el fabricante.	**[34] No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión. Tal como se indica en el considerando, las entidades y empresas supervisadas deben asumir su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados, lo anterior se logra a través	

		de mecanismos de control, tales como cláusulas 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, o aceptación de términos y condiciones de la organización por parte de terceros, o auditorías externas, entre otros.	
	[35]FEDEAC XXII: Se debe considerar que los contratos de adhesión de servicios nube, computo, almacenamiento, etc. son muy estándar y es complejo realizar ajustes sobre los mismos, casi que las organizaciones que requieren de estos servicios deben aceptar los contratos tal cual están definidos por el fabricante.	**[35] No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión. Tal como se indica en el considerando, las entidades y empresas supervisadas deben asumir su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados, lo anterior se logra a través de mecanismos de control, tales como cláusulas 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, o aceptación de términos y condiciones de la organización por parte de terceros, o auditorías externas, entre otros.	
	[36]VIDAPLENA Pregunta XXII 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. Observación/Consulta: En relación con este apartado, lo siguiente: ¿Sería posible asegurar	**[36]No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión. Tal como se indica en el considerando, las entidades y empresas supervisadas deben asumir su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI	

	la confidencialidad y la continuidad en un 100% mediante un contrato de adhesión, con un solo proveedor?	tercerizados, lo anterior se logra a través de mecanismos de control, tales como cláusulas 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, o aceptación de términos y condiciones de la organización por parte de terceros, o auditorías externas, entre otros. La entidad es la responsable de definir con los proveedores por ejemplo los niveles de disponibilidad entre otros aspectos.	
	[37]CB En el Considerando XXII, hay que tener en cuenta que generalmente una empresa no tiene el suficiente músculo para pedir condiciones diferenciadas a proveedores internacionales como Amazon. Por eso aplica el contrato de adhesión.	**[37] No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión. Tal como se indica en el considerando, las entidades y empresas supervisadas deben asumir su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados, lo anterior se logra a través de mecanismos de control, tales como cláusulas 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, o aceptación de términos y condiciones de la organización por parte de terceros, o auditorías externas, entre otros.	
	[38]BCR ¿Cuál es la posibilidad real de la Entidad de asegurar confidencialidad y la continuidad de los bienes y servicios delegados en un tercero mediante la figurade	**[38] No procede** En diferentes partes de la propuesta de modificación reglamentaria se indican aspectos a considerar cuando se trata de contratos de adhesión.	

	un contrato de adhesión?. La cláusula es ambigua. Mientras por una parte reconoce la existencia de contratos de adhesión, por otro lado, exige a la Entidad asegurar condiciones que NO son gobernables por la entidad.	Tal como se indica en el considerando, las entidades y empresas supervisadas deben asumir su responsabilidad sobre el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados, lo anterior se logra a través de mecanismos de control, tales como cláusulas 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, o aceptación de términos y condiciones de la organización por parte de terceros, o auditorías externas, entre otros. La entidad es la responsable de definir con los proveedores por ejemplo los niveles de disponibilidad entre otros aspectos.	
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.	**[39]ISACA** 1-El apartado cuenta con varias fuentes de referencia con varios años de obsolescencia porque la pandemia cambio el panorama. Se debería proporcionar los datos actuales que den sustento al tema de seguridad de la información, que dicho sea de paso debe empezar a educarse en que la seguridad cibernética es parte de la seguridad de la información, ya que en la actualidad se gestionan separados y de hecho la prioridad la tiene la ciberseguridad, donde esta es la menos vulnerable que la seguridad física, legal y administrativa.	**[39] No procede** El Reglamento General de Gobierno y Gestión de TI consideró en su diseño las últimas versiones de las mejores prácticas, estándares, internacionales y marcos de referencia, así como un análisis del derecho comparado en otras legislaciones y se contó con la asesoría del Toronto Centre y el Fondo Monetario Internacional, con el fin de contar con fuentes de referencia actualizadas y validas dentro del contexto de riesgos globales provistos por el Foro Económico Mundial en sus informes de riesgos. Por su parte, el Reglamento General de Gobierno y Gestión de TI en el "Artículo 1. Objeto", indica que la finalidad es establecer los requerimientos para el	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.

	Existe referencia a la seguridad de la información, pero se hace mucho énfasis en riesgo cibernético, riesgos que requieren acciones no cibernéticas para controlar su frecuencia e impacto. En el contexto, se deja de lado la seguridad de la información, se menciona el SGSI pero sin clarificar los ámbitos de la seguridad física, legal y administrativa, ya que sin este gobierno no se podría contar con una seguridad cibernética que perdure en el tiempo y que resista los cambios significativos o las emergencias. 2-¿Cuáles son los criterios para considerar que existe un SGSI, existe una guía como parte de la normativa? ¿Cuál es el grado de automatización que debe tener el SGSI?	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. Además, hace hincapié que el reglamento 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. Po ejemplo, 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. 2-La entidad es la que debe establecer el sistema de gestión de la seguridad de la información, para lo cual podrán 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. El Marco de control interno establecido por las entidades o empresas supervisadas puede ser automatizado o manual. La decisión de llevar controles manuales o automáticos queda a discreción de la entidad, considerando el modelo, tamaño y complejidad del negocio.	
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			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.			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 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.	**[40]BPDC Pregunta** En el apartado XXVIII, ¿el sistema de gestión de SI se debe certificar?	**[40]No procede** En ningún caso el marco de regulación hace referencia que la entidad deba certificarse o deba certificar algún proceso de TI.	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.

	[41]CATHAY Se sugiere incorporar una guía de normativas o marcos de referencia internacionales consultados o sobre los cuales se basa esta normativa. Es importante estar claro en cuales buenas prácticas en materia de seguridad cibernética se basa la normativa. Tal como se indició anteriormente, es importante citar las normativas o marcos de referencia internacionales sobre los que se basa esta normativa.	**[41] No procede** La propuesta de modificación reglamentaria toma como base diferentes estándares internacionales, mejores prácticas y marcos de referencia; no uno solo en particular.	
	[42]CAJAANDE Agradecemos nos puedan aclarar cuál es el termino correcto, si ciberseguridad o seguridad cibernética. XXVII. Agradecemos considerar la posibilidad de que este marco	**[42] 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	

	podría ser un documento individual y no una adhesión, debido a que existen entidades supervisadas que cuenta con nivel de madurez alto y poseen un SGSI, gobierno de Seguridad de la Información y una estructura interna con figuras que van desde un CISO, Comité de seguridad de la Información y procesos maduros en este ámbito, gestionados por un área, departamento o unidad organizacional específica.	términos pueden emplearse de manera equivalente. Independientemente del tamaño de la organización, es crucial gestionar los riesgos de seguridad de la información y seguridad cibernética. Dichos riegos no discriminan por tamaño de la organización; todas están expuestas a amenazas y ataques cibernéticos. Si embargo, dentro de la modificación regulatoria se incorpora el tema de regulación proporcional.	
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.	**[43]COOPEANDE** La implementación de un sistema de seguridad de la información, aunque no conlleve un proceso de certificación, requiere de una serie de recursos humanos, financieros y tecnológicos, por lo que es importante dejar más claro, la posibilidad de que la organización defina el alcance de ese sistema de seguridad de la información con base en su estrategia, contexto y riesgos.	**[43] No procede** Tal como se indica en la regulación, 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. Los estándares internacionales, mejores prácticas o marcos de referencia relacionados con la seguridad de la información y en particular los relacionados con Sistemas de Gestión de Seguridad de la Información establecen que se debe definir el alcance de dicho sistema, en parte según su estrategia, contexto, riesgos y demás particularidades.	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.
	[44]FEDEAC XXVIII: La implementación de un sistema de seguridad de la información, aunque no conlleve un proceso de certificación, requiere de una serie de recursos	**[44] No procede** Tal como se indica en la regulación, para la implementación del sistema de gestión de la seguridad de la información, se pueden utilizar los estándares internacionales, mejores	

	humanos, financieros y tecnológicos, por lo que es importante dejar más claro la posibilidad de que la organización defina el alcance de ese sistema de seguridad de la información con base en su estrategia, contexto y riesgos.	prácticas o marcos de referencia relacionados con la seguridad de la información y la seguridad cibernética que la industria de tecnologías ha desarrollado. Los estándares internacionales, mejores prácticas o marcos de referencia relacionados con la seguridad de la información y en particular los relacionados con Sistemas de Gestión de Seguridad de la Información establecen que se debe definir el alcance de dicho sistema, en parte según su estrategia, contexto, riesgos y demás particularidades.	
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.	**[45]ISACA** El perfil tecnológico debe ser muy sintético, gráfico y conciso. Es en la auditoría externa donde se considera la calificación real, el perfil tecnológico deberá ser sencillo y claro.	**[45] No procede** El Perfil tecnológico es una 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. Los resultados de la Auditoría Externa de TI serán considerados como parte del criterio informado, que se utilizará como insumo de la metodología para determinar la calificación que se establece en las regulaciones particulares de cada Superintendencia y alineadas al modelo de supervisión basada en riesgos.	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), esta reconoce las aptitudes y conocimientos de un profesional en las áreas de auditoría de sistemas de información,	**[46]Luis Diego León Barquero** Yo agregaría al punto XXX, lo siguiente: “En el caso de la certificación Certified Information Systems Auditor (CISA por sus siglas en inglés) emitida por ISACA).”	**[46]Procede** Se ajusta la redacción.	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

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.			de TI, adquisición, desarrollo e implementación de sistemas de información, operaciones, mantenimiento y soporte de sistemas de información y protección de activos de información.
	[47]COOPEFYL Coopefyl atiende lo establecido del Acuerdo Sugef 25-23, y lo dispuesto en el artículo 3 de la presente propuesta de reglamento en consulta. Dado que es discrecional la aplicación de este capítulo II para las cooperativas de ahorro y crédito del del Acuerdo 25-23, y en el artículo 8 inciso c) del capítulo II se establece la contratación de la Auditoría Externa por parte del órgano de Dirección, sin embargo, en el artículo 46 sección II del capítulo V se establece la obligación de la contratación de la Auditoría Externa. Consideramos que hay una contradicción, por un lado, se indica que no es obligante la aplicación del capítulo II y por otro lado, se obliga en el capítulo V artículo 46 sección II la contratación de la Auditoría externa, favor aclarar. Además, en el Anexo 2 de los Lineamientos Generales se establecen los procesos de gestión de TI que deben ser evaluados sin ninguna descripción lo que se reitera la contradicción del artículo 3 de la presente norma y lo establecido en el anexo 2, de los Lineamientos Generales. Como se aplicará para las cooperativas de ahorro y crédito que se encuentran	**[47] No procede** La aplicación de la proporcionalidad de los aspectos indicados en el capítulo II y III, no está en contradicción a los elementos indicados en el capítulo V, ya que las entidades y empresas supervisadas pueden incorporar como sanas practicas los elementos mínimos indicados en los capítulos II y III. Además, se debe considerar que la presente propuesta reglamentaria 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. En virtud de lo anterior, las entidades deberán establecer las medidas de control para mitigar los riesgos relacionados con las tecnologías de información, la seguridad de la información y la seguridad cibernética. A su vez la auditoría externa de TI, por medio de los procesos de evaluación definidos en los anexos, deberán corroborar la gestión de dichos riesgos.	

	en el Acuerdo Sugef 25-23 atender esta contratación, ya que la presente propuesta exime a las cooperativas del marco de gobierno y de gestión de TI, capítulo II y III, y le exime al Órgano de Dirección la contratación de la Auditoría Externa artículo 8 inciso c) y por otro lado deja como obligante la aplicación del artículo 46 sección II Auditoría Externa, en temas que está eximiendo a las cooperativas de ahorro y crédito. Además, en los lineamientos generales Anexo 2 se definen procesos de evaluación de la gestión de TI que será evaluados por la Auditoría Externa sin ningún alcance y en contrario a lo establecido en la presente norma de consulta artículo 3 para las cooperativas que están sujetas a la regulación proporcional.		
	[48]BPDC En el apartado XXX, consideramos que no se debe considerar solo una certificación para validar el conocimiento de un auditor. Se debe considerar al menos 3 años de experiencia comprobada de la auditoría, además, se debe incluir certificaciones de Auditoría de SGSI ISO27001, ISO22301 y de Ciberseguridad de ISACA.	**[48] No procede** a. Los requisitos que deben cumplir las firmas o los profesionales independientes para realizar las auditorías externas de TI están dispuestas a través del el Reglamento General de Auditores Externos, Acuerdo CONASSIF 1-10.	
	[49]CB Sobre la referencia a la Certificación CISA, también se pueden considerar otras certificaciones de Auditoría como	**[49] No procede** Las acreditaciones están establecidas en el Reglamento General de auditores externos, Acuerdo Conassif 1-10. Por lo	

	SGSI ISO27001, ISO22301 y de Ciberseguridad de ISACA.	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.	
	[50]CCPA Es importante mencionar que este servicio de auditoría debe ser prestado por profesionales debidamente incorporados en el Colegio de Contadores Públicos de Costa Rica, (contadores públicos autorizados/CPA), la cual regula el ejercicio de la auditoría conforme a la Ley 1038; y cuya formación se complementa o se especializa a través de certificaciones como la CISA u otras que suele escoger el CPA.	**[50] No 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.	
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 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.			XXXI. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de Costa Rica estableció una Estrategia Nacional de Ciberseguridad con el objetivo de diseñar un marco para orientar las acciones que el país puede tomar con respecto al uso seguro de TI y desarrollar la coordinación y cooperación entre las partes interesadas. El papel del regulador incluye contar con un marco normativo basado en buenas prácticas para la protección de infraestructuras críticas con el fin de desarrollar una infraestructura de monitoreo y alerta temprana para la detección, prevención y respuesta de incidentes de seguridad cibernética.
XXXII. La industria y los profesionales en TI han desarrollado estándares, buenas prácticas y	**[51]Luis Diego León Barquero**	**[51] Procede**	XXXII. ~~La industria~~ Las asociaciones profesionales, entidades globales, gobiernos de diferentes

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.	Yo cambiaría la redacción del punto XXXII, por la siguiente redacción: Las Asociaciones Profesionales, entidades globales y gobiernos de diferentes países industria y los profesionales en TI han desarrollado estándares, buenas prácticas y marcos de referencia para gestionar y controlar las tecnologías…Yo agregaría en punto XXXIII, lo siguiente: "El marco de referencia COBIT 2019 emitido por la Asociación Profesional ISACA…"En el punto XXXIV: yo haría un apartado para los siguientes entes: a. NIST que es una organización del gobierno Federal de los Estados Unidos; b. ISO que es una organización global. c. Center for Internet Security es una Asociación sin fines de lucro. Yo empezaría por la organización ISO, luego la NIST, y de último el Center for Internet Security.	Se incorpora parte de lo indicado en las observaciones.	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 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.	**[52]COOPEFYL Pregunta** Este estándar de TI COBIT versión 2019 es suficiente para atender los temas de seguridad de la información y seguridad cibernética.? ¿O debe complementarse con otro estándar?. ¿Es necesario utilizar este estándar NIST o con la versión COBIT 2019 es suficiente?	**[52]No procede** La selección de cuáles marcos de referencia y estándares utilizar es algo que queda a discreción de la entidad. La adopción de los estándares internacionales, mejores prácticas o marcos de referencia relacionados con la seguridad de la información y la seguridad debe responder a los requisitos, requerimientos y necesidades de las partes interesadas relevantes y estar alineada a los objetivos y estrategias definidas por cada entidad o empresa supervisada.	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.
	[53]BPDC Pregunta	**[53]No procede**	

	En el apartado XXXIII, se consulta: dentro del ámbito y conceptos de COBIT 2019, se evaluará capacidad/desempeño de los procesos o la madurez de áreas de interés? ¿Además, se evaluarán todos los procesos o las organizaciones evaluadas pueden determinar cuáles procesos les aplica? Finalmente se recomienda sustituir COBIT 2019 por "Cobit en su versión más reciente." En el apartado XXXIV, especificar que se refiere a la ISO27001 SGSI.	Se atiende como consulta. Se incluye la respuesta en la sección de preguntas frecuentes ubicada en el sitio web de cada Superintendencia. a. Las entidades o empresas supervisadas pueden adoptar y adaptar los estándares, buenas prácticas y otros marcos de referencia desarrollados por la industria y los profesionales de TI, para fortalecer el control interno de las tecnologías de información. b. La adopción y adaptación de estas prácticas deben estar de conformidad con el principio de proporcionalidad, el modelo, tamaño y complejidad del negocio y los riesgos asociados de cada entidad o empresa supervisada c. En caso de que la entidad decida adoptar CobiT 2019 para el diseño e implementación del marco de gobierno y gestión de TI, la selección de las prácticas queda a discreción de la entidad o empresa supervisada, y debe responder a los requisitos, requerimientos y necesidades de las partes interesadas relevantes y estar alineada a los objetivos y estrategias definidas para mitigar sus riesgos asociados. d. De conformidad con lo dispuesto en el Reglamento General de Gobierno y Gestión de TI en el “Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI”, entre otras disposiciones indica 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, de la misma forma,	

		las prácticas que de forma discrecional la entidad o empresas supervisada establezca que no les aplica, podrá estar revelada en el estudio técnico. Con relación a especificar que se refiere a la ISO 27001, el considerando no asocia a una norma específica ya que existes varias normas ISO que disponen de estándares orientados en materia de seguridad cibernética.	
	[54]CATHAY COBIT 2019 tiene diferencias significativas con respecto a sus versiones anteriores. La normativa estuvo claramente basada en esas versiones anteriores. ¿La expectativa es alinear todos los procesos del Marco de Gestión de TI a COBIT 2019 o hacerlo discrecionalmente en función de criterios basados en gestión de riesgo establecidos por cada entidad?	**[54]No procede** La propuesta de modificación reglamentaria toma como base diferentes estándares internacionales, mejores prácticas y marcos de referencia; no uno solo en particular.	
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 y los Controles CIS del Center for Internet Security.	**[55]CCPA** No objetamos el hecho de utilizar normativa internacional, tomando en cuenta que el trabajo será supervisado por un contador públicos autorizado, como se indica en otras secciones de esta normativa.	**[55] No procede** La propuesta de modificación reglamentaria toma como base diferentes estándares internacionales, mejores prácticas y marcos de referencia.	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, ~~y~~ 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			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.			referencia que la industria de tecnologías ha desarrollado para la implementación del marco de gobierno y de gestión de TI, sin perjuicio del cumplimiento de las disposiciones establecidas en este reglamento.
consideraciones de costo-beneficio			
XXXVI. La evaluación costo-beneficio de la regulación se realiza de conformidad con lo establecido en los artículos 1 y 12 de la Ley Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, Ley 8220 y en los artículos 12, 12 bis, 13, 13 bis y 56 al 60 bis del Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, 37045-MP-MEIC. Dicha regulación indica que la Administración Pública debe realizar un análisis de impacto regulatorio mediante una evaluación costo-beneficio antes de emitir cualquier nueva regulación o reformar las existentes, cuando establezcan trámites, requisitos y procedimientos que deba cumplir el administrado ante la Administración. De dicho análisis se determinó que la regulación no establece ni modifica trámites, requisitos o procedimientos que el administrado deba cumplir ante la Administración Central.	**[56]OPC-CCSS** 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.	**[56] 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 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.	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.
	[57]BCR Pregunta ¿Podrían compartir los resultados del análisis de impacto regulatorio realizado?	**[57] No procede** No es una observación dentro del contexto de la redacción del considerando. 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 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.	

	[58]ACOP Esta Asociación discrepa abiertamente de lo indicado en el considerando 34 y en forma expresa solicita que la Administración realice una evaluación de costo beneficio, con la participación de las Operadoras de Pensiones. Lo anterior, por cuanto establecer estándares internacionales, mejores prácticas en materia de innovación, tecnología y telecomunicaciones, para atender temas de ciberseguridad, gestionar y controlar las tecnologías, realizar auditorías externas de TI y seguridad de la información, implica erogaciones adicionales, que no están ni presupuestadas y mucho menos incorporadas, en la es cuál ida comisión que cobran los Operadoras a los afiliados y pensionados, la cual asciende a 0,35 % anualizada sobre saldo administrado. En virtud de lo anterior y dado los recientes cambios en otras normativas, como son Fondos Generacionales, Reglamento de Gestión de Activos, aporte para el mantenimiento del Conassif y la Supen, Gobernanza de las Inversiones y ahora cambios en las regulaciones de TI, es indudable que se incrementa el costo de regulatorio, el cual no fue considerado en el año 2010 cuando se modificó por última vez el porcentaje de comisión, en la	**[58] 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 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.	

	sesión del Conassif número 847 del 23 de abril del2010.El no revisar la estructura de costos de las Operadoras de Pensiones, de previo a implementar las reformas al reglamento general de gobierno y gestión de TI, tendría una afectación directa de los costos regulatorios, creando un riesgo legal para esas entidades, que podría implicar la imposibilidad material de gestionar adecuadamente la gobernanza de la tecnología, todo en perjuicio de los afiliados y pensionados.		
otras consideraciones	**[59]ISACA** Precisamente es una laguna que ha tenido la normativa del SFN porque no se exige la contabilidad de costos básica para determinar impactos, niveles de servicios, niveles de operación y la implementación de los pilares de la arquitectura empresarial: Seguridad, Riesgo y Continuidad. La contabilidad de costos debe ser exigida sí o sí, ya que todos los procesos relacionados con el costo -beneficio, sin atreverse a decir que todos los 40 procesos del Modelo Cobit dependen del costo-beneficio. Sin este insumo no existe posibilidad de determinar el valor de los sistemas de gobierno y gestión.	**[59] 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 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.	
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	**[60]ABC** Observaciones generales: Con base en las normas del Reglamento propuesto, el órgano supervisor manejará una cantidad importante de información	**[60]No procede** Los aspectos señalados en la observación fueron revisados en cada una las correspondientes secciones o apartados de la matriz de observaciones.	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.	sensible, por lo que resulta importante que se incluyan disposiciones sobre las formas en que las superintendencias protegerán esta información. Asimismo, es importante valorar el impacto que tendrá la propuesta en la innovación y la adopción de nuevas tecnologías, así como en las decisiones de inversión de las entidades en esta materia. Se debe buscar un equilibrio entre la seguridad de la información y la innovación, la cual requiere del aprovechamiento responsable de datos Se sugiere revisar la pertinencia de algunas responsabilidades establecidas en las secciones II, III y IV del Reglamento en virtud del principio de proporcionalidad. Lo anterior debido a que, de conformidad con las facultades definidas por ley, el órgano de dirección tiene funciones asociadas principalmente a la aprobación de políticas, el apetito de riesgo, reglamentos, la estrategia de la entidad, asignar responsabilidades y recursos, entre otros y es responsabilidad de la administración activa su ejecución, además de alinear los procesos, procedimientos, registros a los criterios aprobados por el órgano. En consecuencia, se considera que algunas funciones están utilizando verbos descritos en términos de funciones administrativas y operativas que son más bien responsabilidad del		como la calificación de entidades y empresas supervisadas establecidas por cada Superintendencia.

	Administración, y no del órgano de dirección ni de los comités de apoyo. Por ejemplo, no es competencia del órgano de dirección el aplicar una evaluación, pero sí debe velar porque se establezca, supervisar y conocer los resultados de la evaluación y dimensionar los alcances. En ese sentido, se sugiere una revisión integral de los alcances consignados en esas secciones, para una adecuada asignación de responsabilidades, conforme al rol de cada una de las partes y las mejores prácticas. Para efectos de facilitar la aplicación del acuerdo en cuestión, se recomienda que los lineamientos de la gestión de los procesos sobre la seguridad de la información y la seguridad cibernética, evaluación de las necesidades de las partes interesadas y la estrategia para la resiliencia operativa digital estén contenidas en el marco de gobierno y gestión de TI, donde se delimiten las responsabilidades de las partes involucradas en su ejecución. Aplicando esta recomendación, podría generarse un único artículo de responsabilidades que se homologuen o alineen en estructura y alcance con otros reglamentos vigentes como: CONASSIF 4-16, CONASSIF 12-21 y SUGEF 2-10.Respecto a la gestión del comité de TI, también le aplica el principio de proporcionalidad por lo que se		

	sugiere alinear su gestión al artículo 24 del acuerdo CONASSIF 4-16 Reglamento de Gobierno Corporativo y no concentrar sus funciones en aspectos administrativos que son responsabilidad de la Administración, pero sí es responsabilidad de la Administración el rendir cuentas de la gestión de aplicación del marco de gobierno y gestión de TI que incluyan aspectos como resultados de evaluaciones al proceso, ya sean internas o externas, implementación de la estrategia, indicadores de desempeño, entre otros. Finalmente, es importante mencionar que la normativa no incluye los temas de seguridad física.		
		Se agregar considerando dado 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.	XXXVIII. El Acuerdo Conassif 5-17 es una normativa transversal, que resulta de aplicación para los regulados de la Sugef, la Sugeval, la Supen y la Sugese.

			Considerando que el Conassif que conoce temas de Supen se encuentra parcialmente desintegrado, por estar pendiente el nombramiento del representante de la Asamblea de Trabajadores del Banco Popular y de Desarrollo Comunal, debido a que el nombramiento del señor Álvaro Enrique Ramírez Sancho fue dispuesto por la Junta Directiva del Banco Central de Costa Rica en el artículo 5 de la sesión número 5857-2018 de 12 de diciembre de 2018, por cinco años, concluyendo, como es sabido, el día 14 de diciembre de 2023, es necesario que para los regulados del sector pensiones esta reforma sea adoptada utilizando para ello la teoría del funcionario de hecho.
			Al respecto, y atendiendo a una consulta formulada por Conassif, debido también a la falta de nombramiento del representante de la Asamblea de Trabajadores del Banco Popular y de Desarrollo Comunal, en el criterio C-100-2011 del 3 de mayo de 2011, la Procuraduría General de la República explica que:
			"En el caso que nos ocupa, el Consejo está bien integrado para su funcionamiento general y en relación con otras Superintendencias. Empero, no lo está cuando se trata de conocer asuntos específicos relacionados con la competencia de la Superintendencia de Pensiones. Competencias todas que son indispensables para el correcto funcionamiento no solo de la Superintendencia de Pensiones sino del sistema de pensiones del país en general. Es el caso del ejercicio de la potestad reglamentaria y de la sancionadora y, en general, aquellas en que se manifiesta la regulación del sector pensiones. Importa recalcar que si el Consejo Nacional de Supervisión del Sistema Financiero no se constituye en los términos del artículo 35 de la Ley 7523, no puede conocer de estas facultades en relación con la Superintendencia de Pensiones, con lo que esta no podría actuar sus competencias, satisfaciendo el interés público que justifica su existencia. Con lo cual se arriesgaría, obviamente, el orden público económico que impregna toda la regulación y supervisión del sistema financiero en general y del de pensiones, en particular." [Lo resaltado no es del original].

			No obstante, en dicho criterio se reconoce que: "Resulta incuestionable que el resguardo de los derechos e intereses de los trabajadores beneficiarios del sistema de pensiones, así como la estabilidad y solvencia del sistema financiero en su conjunto requieren la continuidad del funcionamiento del CONASSIF y de la SUPEN. Continuidad que, repetimos, se ve afectada cuando el órgano colegiado, CONASSIF, no está debidamente integrado para conocer de los asuntos regulatorios en materia de pensiones y, por ende, para actuar las competencias respectivas. Consecuencia que puede evitarse con la aplicación de la teoría del funcionario de hecho […]". [Lo resaltado no es del original].
			Ahora bien, la Procuraduría concluye que: "El Consejo Nacional de Supervisión del Sistema Financiero puede recurrir a la figura del funcionario de hecho a efecto de emitir el acto previsto por la Ley, en situaciones de evidente riesgo de ese orden público económico y social". Y agrega: "Es entendido que la actuación del funcionario de hecho debe tender a la satisfacción general y a la concreción de los fines a que se refiere el orden público a que se ha hecho referencia, en particular la protección de los derechos e intereses de los trabajadores garantizados por la Ley de Protección al Trabajador". [Lo resaltado no es del original].
			Se justifica que la propuesta de modificación integral del Acuerdo Conassif 5-17 sea adoptada para los regulados por la Superintendencia de Pensiones, recurriendo para ello a la teoría de funcionario de hecho, por las siguientes razones:
			a) Los ataques cibernéticos representan una amenaza creciente en frecuencia y sofisticación, con impactos disruptivos para la continuidad del negocio y la integralidad de la información, con efectos perjudiciales para la estabilidad de las entidades financieras y del Sistema Financiero Nacional. Esta realidad, evidencia la necesidad imperiosa de que, a nivel reglamentario, se requiera a las entidades financieras un marco robusto de

			gestión del riesgo de seguridad cibernética, teniendo en cuenta, además, el alto grado de interconexión entre ellas y la existencia de entidades de importancia sistémica.
			b) Las vulnerabilidades de seguridad de la información y seguridad cibernética de los proveedores de bienes y servicios de TI podrían convertirse en canales de ataque a las entidades supervisadas, por lo que, las capacidades de seguridad de dichos proveedores son elementos críticos, y se requiere de las entidades supervisadas una gestión diligente de su relación con dichos proveedores.
			c) La computación en la nube tiene beneficios, pero también presenta riesgos potenciales, como los relacionados con la seguridad y la confidencialidad de los datos, así como la vulnerabilidad de los sistemas de tecnología de la información (TI) a los ataques cibernéticos.
			d) Los incidentes e interrupciones de servicios de TI podrían afectar la operación continua de los procesos críticos para el negocio y la disponibilidad de la información de las entidades supervisadas, así como asegurar la continuidad del proceso de supervisión.
			e) La implementación de tecnologías emergentes puede provocar un impacto estratégico en las entidades supervisadas si no se gestionan adecuadamente sus riesgos. Es necesario que la supervisión de TI permita valorar si las entidades están preparadas para aprovechar las ventajas de las innovaciones tecnológicas y gestionar los riesgos asociados.
			Lo planteado anteriormente, evidencia la existencia de riesgos que requieren ser abordados a nivel regulatorio, a efecto de que exista un estándar mínimo que deban observar las entidades financieras en sus operaciones. Claramente, la inadecuada gestión de esos aspectos, así como de otros que están contemplados en el reglamento, tienen la virtud de poder afectar seriamente al sistema financiero, a las entidades mismas, así como al orden público económico y social.
			Finalmente, y por tratarse de una norma transversal, resulta indispensable que la modificación propuesta se apruebe no solo para los regulados por la Sugef, la Sugeval y la Sugese; este cambio debe ser aprobado

			también para los regulados por la Supen con el propósito de asegurar un trato uniforme con el resto de las empresas y entidades supervisadas de los grupos y conglomerados financieros y para evitar los espacios de asimetría regulatoria, que se podrían generar como consecuencia de la aplicación de una regulación desigual entre las entidades supervisadas del sistema financiero, sin que exista una justificación técnica para ello.
			Conviene agregar que, desde larga data, la Sala Constitucional se ha pronunciado sobre la validez de las actuaciones emanadas de los funcionarios de hecho, de cumplirse los presupuestos establecidos en las normas atinentes de la Ley General de la Administración Pública. Así, en el voto 1593-94 indicó que:
			"Esta Sala ha aceptado válidamente, la aplicación de la teoría del funcionario de hecho, estipulada en la Ley General de la Administración Pública, en sus artículos 155 y siguientes. En reiteradas ocasiones, (vid sentencias N.° 2765-92, 15:30 horas del 01-09-92 y N.° 6701-93, 15:06 del 21-12-93) ha manifestado que las actuaciones realizadas por un funcionario de hecho, revisten su carácter de validez en tanto se cumplan determinados requisitos o condiciones, ello con la necesidad de preservar el interés general, mismo que constituye el principal objetivo que ha de ser atendido por el ordenamiento jurídico. Por lo que acerca de los requisitos para reconocer la validez de los actos de los funcionarios de hecho, se encuentra este tribunal los siguientes:
			´ ... Que exteriormente se presenten como si emanaran de funcionarios de jure, es decir, deben producir, respectos a terceros, al público, los efectos jurídicos propios de los actos que emanan de agentes verdaderamente regulares... El reconocimiento de la validez de esos actos en favor de los terceros, debe ser "de interés público", en busca de la seguridad jurídica y la certidumbre del derecho... También es necesario que lo actuado por el funcionario de hecho se haya realizado dentro de los límites de competencia de la autoridad oficial que dicho funcionario pretende tener...´

			(Sentencia número 6701-93)". [Lo resaltado no es del original].
			Por su parte, en el criterio C-100-2011, arriba mencionado, la Procuraduría General de la República reafirma el carácter de interés público de que revista la regulación financiera, como sigue:
			"El carácter de interés público de la regulación financiera es indiscutible y se origina en el hecho mismo, repetimos, que las entidades financieras actúan en el mercado, captando, manejando, invirtiendo el ahorro de terceros. De allí la necesidad de regular que las entidades no incurran en riesgos que lesionan el interés de los ahorrantes o inversionistas.
			Por ese poder de policía de contenido financiero, se permite a los órganos regulador y supervisor reglamentar la actividad financiera y los agentes que en ella intervienen, dictando normas que permiten interpretar e integrar las leyes en la materia, vigilar el funcionamiento del sistema y aplicar esas leyes; en su caso, sancionar el irrespeto al régimen especial. De esa forma, se orienta y dirige la actividad financiera necesaria para atender las necesidades de la producción y el consumo, así como satisfacer los intereses de los inversionistas o ahorrantes. Importa destacar que se reconoce la posibilidad de imponer reglas de comportamiento a los intermediarios financieros, tendientes a prevenir que incurran en riesgos excesivos y a garantizar la solvencia y la liquidez de los establecimientos. El objetivo último: la estabilidad y solvencia de los distintos agentes financieros y del sistema en general". Dictamen N. C-320-2005 de 6 de setiembre de 2005.
			A la estabilidad y solvencia de los entes supervisados por la Superintendencia de Pensiones, se une la finalidad social propia del régimen de pensiones, que no es otra que la protección del trabajador y ex trabajador en caso de invalidez, vejez y muerte. […]" [Lo resaltado no es del original].
		Se agregar considerando para indicar que la propuesta de modificación reglamentaria fue enviada en consulta.	XXXIX. Mediante artículos 4 y 5 de las actas de las sesiones 1834-2023 y 1835-2023, celebradas el 20 de noviembre del 2023, el Conassif remitió a consulta pública la propuesta de modificación al

			Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17, en el entendido que, en un plazo máximo de quince días hábiles, contados a partir del día hábil siguiente del recibo de la respectiva comunicación, las entidades del Sistema Financiero Nacional podían enviar al Despacho de la superintendente general de entidades financieras sus comentarios y observaciones. Posteriormente, mediante artículos 6 y 4 de las actas de las sesiones 1837-2023 y 1838-2023, celebradas el 4 y 6 de diciembre del 2023, el Conassif dispuso extender, al 15 de enero del 2024, el plazo para la recepción de comentarios y observaciones a la citada propuesta de modificación normativa remitida en consulta.
dispuso:			**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.	**[61]FEDEAC** Las entidades deben definir la gradualidad de implementación de este reglamento y de los lineamientos de acuerdo con su grado de madurez, tamaño, apetito de riesgo y estrategia.	**[61] 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.	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
	[62]COOPEALIANZA Se solicita modificar el nombre del reglamento al siguiente: REGLAMENTO DE GOBIERNO Y GESTIÓN EMPRESARIAL PARA LA	**[62] No procede** La propuesta de modificación reglamentaria toma como base diferentes estándares internacionales, mejores prácticas y marcos de referencia; no uno solo en particular.	

	INFORMACIÓN Y LATECNOLOGIA, 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.		
	[63]ISACA Se deberá identificar los puntos de control de dicha integración y complementariedad entre las normas de REGLAMENTO GENERAL DE GOBIERNO Y GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN y El Reglamento de Gobierno corporativo.	**[63] No procede** Sin perjuicio de las disposiciones contenidas en la presente propuesta de modificación reglamentaria, las entidades deben cumplir con la regulación aprobada por el CONASSIF, entre ellas el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16. Por lo tanto, los aspectos de responsabilidades asignadas a los Órganos de Dirección, Alta Gerencia y Órganos de control incorporados en la presente modificación reglamentaria complementan lo ya dispuesto en el Acuerdo CONASSIF 4-16, pero con un enfoque específico haca temas de TI. Los considerandos del presente reglamento entre otros aspectos indican que el gobierno de la tecnología de información es una parte fundamental del gobierno corporativo, por lo tanto, los mecanismos de control relacionados con los procesos de gobierno del marco y el reglamento de gobierno corporativo pueden ser identificados por parte de las entidades y empresas supervisadas a través del estudio técnico indicado en el "Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI"	

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.			La presente regulación se tendrá como plenamente integrada y complementaria al marco general de gobierno y de gestión de riesgos establecido en el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16 y en el marco de regulación vigente sobre gestión de riesgos de cada Superintendencia.
Artículo 2. Alcance			**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.			e) Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados.
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:	**[64]COOPEFYL** Se exime a las cooperativas de ahorro y crédito sujetas a la Regulación Proporcional según el Acuerdo Sugef 25-23 de la aplicación de este capítulo II, GOBIERNO y GESTIÓN TI, se realiza el comentario que son referencias que discrecionalmente	**[64] 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	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:

	podrán adoptar las entidades. Por lo tanto, no queda claro cómo queda la aplicación de los lineamientos generales ANEXO 2 sobre la gestión de TI y la definición del perfil tecnológico según artículo 42 del capítulo V y la realización de la Auditoría Externa ya que se indican proceso de gestión de TI a evaluar por las cooperativas que se encuentran en la proporcionalidad. ¿Se exime o no a las cooperativas del Gobierno y gestión de TI o no? Como que lo establecido en el Anexo 2 de los Lineamientos Generales y además se desconoce los alcances o descripción de los procesos se enumeran en dicho apartado. El eximir de la aplicación de este capítulo III al igual que el capítulo II, como se atenderá el tema de la Auditoría Externa artículo 46 del Capítulo V. Asimismo, deben indicar como se alinea el tema de la aplicación de los Lineamientos Generales Anexo 2 para la realización de la Auditoría Externa con lo establecido en los artículos que se está eximiendo en la presente propuesta. Favor referirse a estos temas para comprender ampliamente. Se indica que del Capítulo IV los artículos 33, 34 y 35 no aplican o son discrecionales. Sin embargo, se mantiene en aplicación los artículos 31 y 32 de esta sección 1, que están relacionados con los marcos de gobierno de TI, marco	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.	

	de gestión de TI que son discrecionales para las cooperativas que se encuentran en el Acuerdo Sugef 25-23.? Además, esto se refuerza en el Anexo 2 de los Lineamientos Generales de los procesos de gestión de TI a evaluar por la Auditoría Externa, con lo cual debe aclarar si se exime o no a las cooperativas sujetas a la regulación proporcionales ya que entre los Lineamientos Generales del anexo2 y los artículos que no son obligatorios hay discrepancias. En este capítulo V se exime o es discrecional los artículos 43, 44 y el inciso b) del artículo 47. Sin embargo, en el mismo artículo 47 Alcance y plazo de la auditoría externa de TI, en el inciso a se menciona: "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.", nuevamente se exime la aplicación del capítulo II y III, pero en este artículo se menciona que se aplica, ¿favor aclarar esta situación? o revisar si se mantiene ese inciso a.? El alcance de la Auditoría Externa según establece en el anexo 2 de los Lineamientos Generales para las cooperativas que están sujetas al Acuerdo Sugef 25-23, se mencionan los procesos, no se incluye ninguna descripción		

	o alcance, y esto no tiene relación con el planteamiento del presente reglamento que exime a las cooperativas de los capítulos I y II. Favor aclarar. ¿A partir de que fecha se define este plazo de 3 años? ¿La SUGEF establecerá algún cronograma como lo realizó en la 5-17? ACUERDO SUGEF 25-23: REGULACIÓN PROPORCIONAL PARA COOPERATIVAS DE AHORRO Y CRÉDITO SUPERVISADAS Artículo 5. Aplicación del marco de regulación El Reglamento sobre Gobierno Corporativo, Acuerdo Conassif 4-16, el Reglamento sobre idoneidad y desempeño de los miembros del órgano de dirección y de la alta gerencia de entidades y empresas supervisadas, Acuerdo CONASSIF 15-22, y el Reglamento sobre Administración Integral de riesgos, Acuerdo SUGEF 2-10, no serán de cumplimiento obligatorio para las entidades sujetas a esta regulación, sino que se considerarán como referencias sobre sanas prácticas.		
	[65]FEDEAC Pregunta Para las organizaciones con regulación proporcional, a quienes las Unidades de Riesgos ya no son obligatorias, ¿cómo se interpreta la permanencia defunciones de riesgos tecnológicos, de seguridad de información, seguridad cibernética y de continuidad? ¿Será necesario mantener dichas	**[65]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	

	Unidades o sus Oficiales con independencia de la Unidad de TI?	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.	
	[66]COOPEBANPO Pregunta Para las organizaciones con regulación proporcional, a quienes las Unidades de Riesgos ya no son obligatorias, ¿cómo se interpreta la permanencia de funciones de riesgos tecnológicos, de seguridad de información, seguridad cibernética y de continuidad? ¿Será necesario mantener dichas Unidades o sus Oficiales con independencia de la Unidad de TI?	**[66]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.	
	[67]COOPESERVIDORES Aclarar, cuál es la interpretación de las Corredoras de S.A. que pertenecen a Grupos financieros y, la gestión de tecnologías se ha definido como Corporativa. O, si este alcance, es solo cuando corresponde a Corredoras como empresa individual sin pertenecer a un Grupo.	**[67]No procede** Se atiende como consulta. Las corredoras que están incorporadas dentro de un grupo o conglomerado financiero, y cuyos servicios de TI y su gestión es tipificada como corporativa, les aplica el Marco de Gobierno y Gestión de su casa matriz.	
	[68]ACOP ACOP propone que se desarrolle una regulación proporcional como la que se indica en el artículo 3 para las Cooperativas de Ahorro y Crédito y para las Sociedades Corredoras de Seguros, dado que al igual que esas entidades no tienen la fortaleza financiera de otros sujetos regulados en esta normativa que se propone modificar.	**[68]No procede** Las entidades miembros de ACOP son mucho más complejas y administran montos mucho mayores que las entidades sujetas al artículo 3 de la presente modificación reglamentaria.	
	[69]CIS Se reconoce la importancia del proyecto normativo, la exposición a riesgo del sector y la necesidad	**[69]Procede** Se modifica la gradualidad en las disposiciones transitorias para	

	de inversión, pero se sugiere considerar características del sector para ir alcanzando un nivel intermedio y de ahí avanzar a un nivel alto y no alto desde inicio, para un desarrollo paulatino. En la Banca se viene avanzando desde 2009 y a hoy incluso algunos procesos siguen en desarrollo; en Aseguradoras se viene trabajando desde 2017 en el tema. Interesa conocer hoja de ruta del modelo de supervisión y regulación para el sector de intermediación, dada la diversidad de participantes, siendo este un actor por revelar al supervisor con el fin de que sea considerado en la probabilidad de éxito efectivo de las propuestas regulatorias y los objetivos planteados. Máxime tratándose de temas en constante transformación, un tema permanente en la actualidad. - No son normas de cumplimiento, sino que tienen impacto en modelo de negocio, estructura, gobernanza, gestión de riesgos, toma de decisiones, contrataciones. Esfuerzo metodológico. - Necesario análisis de la realidad de los negocios: Ingresos son por comisión, limitaciones presupuestarias, costos no trasladables, sino necesariamente aporte de socios. Se realizó una encuesta a nivel de mercado con resultados muy variados: o Modelos de negocio, diversidad de estructuras organizacionales, diverso grado de madurez de	sociedades corredoras de seguros de tres a cuatro años. Adicionalmente, se incluye en la sección de preguntas y respuestas. Respuesta: La aplicación de la proporcionalidad indicada por el reglamento SUGEF 25-23, implica que las entidades y empresas supervisadas pueden incorporar estos aspectos como sanas prácticas, en función de los riesgos identificados por la entidad. Además, se debe considerar que la presente propuesta reglamentaria 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. En virtud de lo anterior, queda a discreción de la entidad o empresa supervisada, responder a los requisitos, requerimientos y necesidades de las partes interesadas relevantes y estar alineada a los objetivos y estrategias definidas para mitigar los riesgos relacionados con las tecnologías de información, la seguridad de la información y la seguridad cibernética, incluyendo los aspectos de gobierno de TI, incluyendo el diseño de su estructura organizacional para estos aspectos.	

	marcos de gobierno corporativo, tamaño, capacidad de infraestructura, de recursos disponibles o accesibles en materia de TI; inversión inicial es alta. o Necesidad de desarrollo de conocimientos, habilidades y competencias a todo nivel en la organización: necesidad de cultura y madurez (otros sectores no han culminado el proceso). Por ello, en temas de gobernanza que están previstos como de "criterios de referencia y a discrecionalidad" es relevante verificar que el entendimiento es contar con la función o gestión adecuada y proporcional del riesgo, más no aplicar cada rol previsto, porque la mayoría de las estructuras no alcanza ni soporta la cantidad de recursos necesarios. o En muchas organizaciones se debe comenzar por la identificación del sistema de información que utilizan y el uso de la tecnología en sus negocios; identificación y clasificación de la información que manejan, etc. Muchos servicios son tercerizados y se tienen contratos vigentes con diversas fechas de vencimiento, contratos de adhesión, limitada capacidad de verificación de requisitos, costo, limitada capacidad de negociación. Por ende, una alternativa es otorgar mayor discrecionalidad en la exigencia de certificaciones y requisitos de esos proveedores y procurar combinaciones entre proveedores. - Se requiere tiempo		

	para responder a esas necesidades que ameritan consideración previa a la implementación de la regulación para tener el perfil de TI. Es primera exposición a este proceso, no hay experiencia ni nada avanzado, Por ende, las sociedades corredoras irán avanzando en la implementación de los 9 modelos correspondientes asumiendo una hoja de ruta y plan de acción responsable, sin que por ello pueda garantizarse que todas las empresas lograrán estar al nivel de capacidad requerido al cabo de 3 años posteriores a la vigencia de la regulación. Para las organizaciones con regulación proporcional, a quienes las Unidades de Riesgos ya no son obligatorias, ¿cómo se interpreta la permanencia de funciones de riesgos tecnológicos, de seguridad de información, seguridad cibernética y de continuidad? ¿Será necesario mantener dichas Unidades o sus Oficiales con independencia de la Unidad de TI? Se agradece confirmar que la frase "... referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades...." implicará una aplicación proporcional de los marcos de gobierno corporativo, ajustados al nivel de riesgo, complejidad, volumen de negocio, etc, , es decir, que se evaluará la identificación de roles y funciones más no necesariamente la estructura		

	exigida a entidades más sofisticadas.		
	[70]ISACA Las entidades no deberían contar con discrecionalidades porque no son distintas, las entidades financieras se caracterizan, y así la tecnología financiera lo comprueba, en que realizan la misma operación de intermediación financiera y sus productos y servicios hasta pueden ser homologados entre las otras entidades. ¿No se comprende por qué los artículos 33, 34 y 35 no son de aplicación plena, a que se refiere eso? Precisamente son objetivos de control que deben estar estandarizados y de aplicación en un nivel de capacidad óptimo. He insistido en los diferentes foros sobre la materia, que el Modelo Cobit ofrece 40 proceso y algunos de ellos requieren que, si capacidad y madurez estén en el nivel más alto, ya que se consideran procesos maestros, es decir que los demás procesos dependen de forma indirecta o directa de esos procesos maestros. La definición de un alcance en función del perfil de riesgos y de la naturaleza de las operaciones podría ser válido para entidades con niveles de cumplimiento óptimos y una vez hayan demostrado que mantienen los controles y el perfil de riesgos adecuadamente por un lapso de 4	**[70] No procede** Las entidades varían en naturaleza jurídica, tamaño, perfil de riesgo, enfoque de negocio, volumen y complejidad de sus operaciones. Además, se modifica la redacción para aclarar que lo indicado en los artículos 33, 34 y 35 del presente reglamento, se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades, en función de sus riesgos, tamaño, complejidad y modelo de negocio. Los procesos de evaluación del marco de gobierno y gestión dispuestos en los anexos de los lineamientos que acompañan al presente reglamento establecen las expectativas de control, las entidades y empresas supervisadas en función de sus riesgos, tamaño, complejidad y modelo de negocio, podrán optar por implementar estándares, marcos de referencia y mejores prácticas tales como, pero no limitadas a CobiT, por tanto, no se dispone de requisitos puntuales sobre madurez o capacidad de procesos, ya que estos pueden variar según la naturaleza y apetito de riesgos de la entidad o empresa supervisada, cambiando el paradigma de cumplimiento normativo a un paradigma de gestión basada en riesgos. Además, se aclara en la sección de preguntas frecuentes ubicada en el sitio de cada Superintendencia lo siguiente: a. Las entidades o empresas supervisadas pueden adoptar y adaptar los estándares, buenas prácticas y otros	

	revisiones internas trimestrales, una vez que hayan cumplido el primer año, se podría considerar una definición del alcance de la auditoría menor o distinto al alcance general. ¿Acaso los bancos no tienen una misma naturaleza, al igual que entre las cooperativas, incluso las corredurías de seguros no la tienen? Además, este privilegio se puede perder, con la materialización de un riesgo no contenido en el proceso habitual y que su causa raíz estaría oculta, poca transparencia, inadecuada identificación de riesgos y principalmente por la inadecuada definición de procesos y sus controles compensatorios (los que se han dispuesto para nivelar u homologar servicios tecnológicos financieros). El artículo 3.3.b es inconsistente con el artículo 48, aunque se insiste que las auditorías deben ser anuales.	marcos de referencia desarrollados por la industria y los profesionales de TI, para fortalecer el control interno de las tecnologías de información. b. La adopción y adaptación de estas prácticas deben estar de conformidad con el principio de proporcionalidad, el modelo, tamaño y complejidad del negocio y los riesgos asociados de cada entidad o empresa supervisada. c. Considerando lo anterior, la definición y establecimiento de modelos de capacidad o madurez por parte de las entidades y empresas supervisadas deben responder a los requisitos, requerimientos y necesidades de las partes interesadas relevantes y estar alineada a los objetivos y estrategias definidas para mitigar los riesgos relacionados con las tecnologías de información, la seguridad de la información y la seguridad cibernética, incluyendo los aspectos de gobierno y gestión de TI. Finalmente, se aclara que el plazo de 3 años definido en esta disposición fue eliminado.	
1.Lo dispuesto en los capítulos que se indican a continuación se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades:			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.			a) Capítulo II Gobierno y Gestión de TI.
b) Capítulo III Organización de las tecnologías de información.			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 el artículo 33. Programas de análisis de	**[71]ISTMO** Inciso 2) Las sociedades corredoras son una de las principales fuentes de información	**[71] No procede** Si bien los programas de análisis de vulnerabilidades y pruebas son cruciales para la mayoría de las organizaciones, su	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 el artículo 33. Programas de análisis de

vulnerabilidades y pruebas, en el artículo 34. Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de seguridad cibernética y en el artículo 35.Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética, del presente reglamento.	y manejan información sensible que es brindada por los asegurados a las sociedades corredoras y luego éstas lo trasladan a las aseguradoras, son parte de la cadena de manejo de información fundamental en el negocio. Debe aplicarse los artículos 33 y 34, sino no tiene sentido que solo una parte de la cadena de manejo de información (las aseguradoras) deban cumplirlo. A nuestro juicio queda un vacío sobre este punto.	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.	vulnerabilidades y pruebas, en el artículo 34. Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de seguridad cibernética y en el artículo 35.Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética, del presente reglamento.
		Se agrega un párrafo para mejorar el entendimiento de la disposición.	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 el artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI, en el artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética y en el inciso b) del artículo 47. Alcance y plazo de la Auditoría Externa de TI. Además, deben considerarse los aspectos siguientes:			3.Lo dispuesto en el Capítulo V La auditoría externa de TI, será de aplicación plena, salvo lo dispuesto en el artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI, en el artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética y en el inciso b) del artículo 47. Alcance y plazo de la Auditoría Externa de TI. Además, deben considerarse los aspectos siguientes:
a) Las entidades, en función de su perfil de riesgo y de la naturaleza de sus operaciones, definirán el alcance de la auditoría externa estableciendo los procesos de evaluación que consideren pertinentes, según el anexo 1 de los lineamientos generales del presente reglamento. Sin perjuicio de lo anterior, el alcance de la auditoría externa deberá incluir, al menos, los procesos de evaluación que se especifican en el anexo 2 de los lineamientos generales del presente reglamento.	**[72]BCR** 3. a) Actualmente, el alcance de la auditoría externa está compuesto por los requerimientos solicitados por el Supervisor en el oficio respectivo, aclarar si el oficio de solicitud de auditoría externa solamente contendrá la instrucción de realizar la auditoría externa, y será la Entidad quien defina los requerimientos	**[72] No procede** Las entidades definirán el alcance de la auditoría externa considerando como mínimo los 9 procesos para las Sociedades corredoras de seguros y los 13 para las entidades sujetas al alcance del Acuerdo SUGEF 25-23. El supervisor podrá incluir en el oficio dichos procesos señalando que son los mínimos.	*Además, ~~deben considerarse los aspectos siguientes:~~ las entidades, en función de su perfil de riesgo y de la naturaleza de sus operaciones, deberán gestionar TI y sus riesgos relacionados. A fin de evaluar dicha gestión, las entidades deben considerar los siguientes aspectos:* *a) Las entidades definirán el alcance de la auditoría externa estableciendo los procesos de evaluación que consideren pertinentes en función de sus riesgos y modelo de negocio, según el anexo 1 de los lineamientos generales del presente reglamento.*

			b) Sin perjuicio de lo anterior, el alcance de la auditoría externa deberá incluir, al menos, los procesos de evaluación que se especifican en el anexo 2 de los lineamientos generales del presente reglamento.
b) La solicitud de la auditoría externa será cada tres años, excepto cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de anticiparla o aplazarla.	**[73]CB** El sub inciso b) del artículo 3 establece que la solicitud de la auditoría externa será cada 3 años; sin embargo, en el artículo 48 indica que será cada dos años. Se solicita revisar y armonizar estas normas.	**[73] No procede** Se aclara que el plazo de 3 años definido en esta disposición fue eliminado.	~~b) La solicitud de la auditoría externa será cada tres años, excepto cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de anticiparla o aplazarla.~~
Artículo 4. Definiciones y abreviaturas			**Artículo 4. Definiciones y abreviaturas**
Para efectos de este reglamento y sus lineamientos generales, se utilizan las siguientes definiciones y abreviaturas:	**[74]Luis Diego León Barquero** Falta la definición de Gobierno de TI. En la definición de Gestión de TI, se indica "Estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la tecnología de la información...". Sin embargo, el papel de la dirección es de gobierno corporativo. Debe revisarse esta definición. La definición de ISACA Global está desactualizada, pues en la actualidad no significa nada. En el sitio Web se puede ver lo siguiente: ISACA Global: ISACA es una asociación profesional global y una organización de aprendizaje con 170.000 miembros que trabajan en campos de la confianza digital, como seguridad de la información, gobernanza, garantía, riesgo, privacidad y calidad. Con presencia en 188 países y con 225	**[74] Procede** Se ajustan las definiciones considerando parte de las observaciones. 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:

	capítulos en todo el mundo, ISACA es reconocida alrededor del mundo por su orientación, credenciales, educación, capacitación y comunidad. Para servir a su comunidad profesional en todo el mundo, ISACA ha establecido tres oficinas con sede en América del Norte, Europa y China. Se ha definido marco de gestión de TI, pero no se define el marco de gobierno de TI Falta da definición de Seguridad de la Información. Se define Seguridad cibernética, pero no se define ciberespacio. No entiendo la diferencia entre la definición de Seguridad cibernética y la seguridad de la información. Falta la definición de servicios de computación en la nube.		
	[75]BPDC 1) No existe claridad si el concepto de "impacto significativo" es asignado según el criterio de cada entidad. 2) El adjetivo "críticos" asociado a TI prácticamente engloba a todos, sin hacer diferencia cual es el criterio de "no criticidad". 3) La descripción del concepto es general, por ende, no está asociado a servicios, ni bienes críticos. 4) No existe claridad si los mecanismos alternos de trabajo no basados en tecnología serán siempre válidos en la gestión de la continuidad del negocio.	**[75]No procede** El concepto de impacto significativos debe ser asignado por cada entidad de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos. 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 internacionales y marcos de referencia aplicables a la industria de las TI. En todo caso deben estar documentas a nivel de la organización todas las políticas, procedimientos, instructivos y	

		formularios que permitan sistematizar y repetir dichos análisis como parte de sus procesos de negocio. Por su parte las entidades y empresas supervisadas son las responsables de establecer los mecanismos dentro de sus planes alternos de trabajo para atender posibles situaciones contingentes, en este sentido, dichos mecanismos de control deberán estar diseñados, implementados y probados de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos.	
	[76]MUCAP 1) No existe claridad si el concepto de "impacto significativo" es asignado según el criterio de cada entidad. 2) El adjetivo "críticos" asociado a TI prácticamente engloba a todos, sin hacer diferencia cual es el criterio de "no criticidad". 3) La descripción del concepto es general, por ende, no está asociado a servicios, ni bienes críticos. 4) No existe claridad si los mecanismos alternos de trabajo no basados en tecnología serán siempre válidos en la gestión de la continuidad del negocio.	**[76] No procede** El concepto de impacto significativos debe ser asignado por cada entidad de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos. 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 internacionales y marcos de referencia aplicables a la industria de las TI. En todo caso deben estar documentas a nivel de la organización todas las políticas, procedimientos, instructivos y formularios que permitan sistematizar y repetir dichos análisis como parte de sus procesos de negocio. Por su parte las entidades y empresas supervisadas son las responsables de	

		establecer los mecanismos dentro de sus planes alternos de trabajo para atender posibles situaciones contingentes, en este sentido, dichos mecanismos de control deberán estar diseñados, implementados y probados de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos.	
	[77]FEDEAC i): Se recomienda modificar la redacción de la siguiente forma: "Persona física o jurídica que provee bienes o servicios de TI críticos a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados)", considerando que los bienes y servicios de TI críticos son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación. j): ¿La resiliencia operativa digital se considera como parte de la continuidad de negocio, o se separan la Continuidad de TI (Resiliencia operativa digital) y la Continuidad de Negocio? k): No se encuentra la definición de seguridad de la información, solo se indica la definición de seguridad cibernética. No son lo mismo, y esto puede provocar	**[77]No procede** Al incluir en la definición a los proveedores de bienes o servicios críticos que proveen bienes o servicios relacionados con TI, se busca que las entidades y empresas supervisadas a través de su Sistema de Gestión de Seguridad de la Información y de su Marco de Administración Integral de Riesgos atiendan los riesgos que existen en la cadena de proveedores que gestionan la información que está en custodia de las entidades y empresas supervisadas. Por otra parte, la resiliencia operativa es la capacidad de una organización para resistir una disrupción repentina y recuperarse. Antes, ese concepto era sinónimo de continuidad del negocio o recuperación de desastres. Pero gracias a la digitalización de los negocios, la resiliencia operativa se convirtió en algo más profundo: una mezcla de continuidad del negocio, gestión de riesgos de proveedores, ciberseguridad y más. Considerando lo anterior, las entidades y empresas supervisadas son las responsables de establecer los mecanismos de control de conformidad	

	confusión a la hora de conocer el alcance y responsabilidades propias de seguridad de la información que no solo vela por el activo digital (TI).	con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos. Finalmente, para lo señalado en el punto k); 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.	
	[78]CATHAY Es conveniente definir a nivel del reglamento qué se entiende por un incidente de seguridad cibernética y el alcance que este tiene en cuanto al reporte a la Superintendencia. Es decir, si este incluye ataques cibernéticos efectuados a clientes o si por el contrario solo aquellos que tienen una incidencia directa parala organización.	**[78]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. Adicionalmente, en la sección II, se aclaran los aspectos relacionados con la gestión de los incidentes de seguridad cibernética relacionados con la entidad o empresa supervisada.	
	[79]CFBNCR Se sugiere incluir las definiciones de Instrumentos de adhesión, Gestión de Riesgos tecnológicos, Procesos Críticos, Seguridad de la Información, incidente de seguridad de la información, Activo de información (tangible e intangible), extendido" o "no recuperable".	**[79]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.	
	[80]ABC Es necesario incluir una definición para el concepto "computación en la nube" especificando si aplica	**[80] No procede** En el reglamento se incluyen las definiciones que se requieren destacar dentro del contexto de la propuesta reglamentaria, evitando aquellas que son	

	para nube interna, externa, pública, privada y/o híbrida. En cuanto al inciso i (proveedores de bienes y servicios de TI críticos), se requiere precisar que dicho concepto no abarca el supuesto de la casa matriz u otra sucursal fuera del país del mismo grupo, regional o internacional. Se sugiere incluir las definiciones de Instrumentos de adhesión, Gestión de Riesgos tecnológicos, Procesos Críticos, Seguridad de la Información, incidente de seguridad de la información, Activo de información (tangible e intangible), extendido" o "no recuperable".	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.Cada empresa de un grupo o conglomerado financiero, o de un grupo de interés económico que brinde un servicio a cualquier empresa de su mismo grupo o a un tercero debe ser considerado y tratado como un proveedor por ser cada una de ellas entidades o empresas de naturaleza económica distinta.	
	[81]OPC-CCSS A lo largo del RGGTI se hace referencia al "Marco de gobierno y gestión de TI" pero en las definiciones viene solamente "Marco de gestión de TI", entonces se considera que debe incluirse bien el concepto en dicha sección. Además, incluir conceptos nuevos que se mencionan como vectores de ataque, defensa en profundidad, computación en la nube (y sus tipos), datos en reposo, confianza cero, necesidad del mínimo conocimiento, metas de sustentabilidad, metas de integridad, ciclos del negocio, gobernanza y ecosistema, activos primarios, etc., para eliminar todo tipo de ambigüedad.	**[81 Procede** Se ajusta la redacción para considerar el marco de gobierno y gestión de TI. 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.	
	[82]CB	**[82] No procede**	

	Inciso a: Comentarios: Sobre el concepto de "impacto significativo" se entiende que esto será asignado según el criterio de cada entidad. Inciso h: Inciso i: Comentarios: La descripción de los conceptos de procesos "críticos" y proveedores "críticos" resultan muy generales, de tal forma que no están asociados a servicios, ni bienes críticos. En tal sentido, resulta necesario que se incluyan las definiciones de Instrumentos de adhesión, Gestión de Riesgos tecnológicos, Procesos Críticos, Seguridad de la Información, Activo de información (tangible e intangible), extendido" o "no recuperable". Asimismo, se sugiere incluir en la definición de Seguridad de la Información, que ésta protege los datos indistintamente de su formato físico, digital y contenido y cambiar "Seguridad Cibernética" por "Ciberseguridad" dado que es un término más conocido y utilizado.	El concepto de impacto significativos debe ser asignado por cada entidad de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos. 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 internacionales y marcos de referencia aplicables a la industria de las TI. En todo caso deben estar documentas a nivel de la organización todas las políticas, procedimientos, instructivos y formularios que permitan sistematizar y repetir dichos análisis como parte de sus procesos de negocio. Por su parte las entidades y empresas supervisadas son las responsables de establecer los mecanismos dentro de sus planes alternos de trabajo para atender posibles situaciones contingentes, en este sentido, dichos mecanismos de control deberán estar diseñados, implementados y probados de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos.	
	[83]BCR • Inciso m) Unidad de TI o función equivalente: indicar cuáles procesos del marco de gobierno y gestión de I&T, consideran son los que se ejecutan en la unidad de TI.	**[83]No procede** Según se establece en el artículo "Artículo 43 Procesos de evaluación del marco de gobierno y gestión de TI", las entidades y empresas supervisadas deben indicar en el perfil tecnológico	

	• Se recomienda incluir el concepto de gobierno corporativo, marco de gobierno y gestión de I&T .• Se recomienda incluir el concepto de resiliencia operativa digital. Nuestra recomendación es para que la institución tenga claridad del significado y alcance, ya que con esto se pueden ejecutar las acciones necesarias para su cumplimiento.	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. Se ajustó la redacción de la definición de "marco de gestión de TI para incluir gobierno. La definición de resiliencia operativa digital ya está incluida en la propuesta de modificación reglamentaria.	
	[84]CCPA El Colegio de Contadores Públicos de Costa Rica, considera importante se incluyan las definiciones de conceptos como Marco de gobierno de TI, Seguridad de la Información, Ciberespacio y Servicios de computación en la nube, para adecuada definición de alcance o responsabilidades.	**[84] Procede** Se ajustó la redacción de la definición de "marco de gestión de TI para incluir gobierno. 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.	
		Se incluye la definición para atender parte de la observación 142, punto 3.	**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) Bienes y servicios de TI críticos: Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación.			**b)~~a)~~ Bienes y servicios de TI críticos:** Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación.
b) 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			**c)~~b)~~ 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.			supervisada para proteger sus activos de información, basándose en la evaluación de riesgos.
c) Gestión de TI: Estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la tecnología de la información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.		Se ajustó la redacción de la definición para mejorar su claridad.	**dc) Gestión de TI:** Conjunto de estructura de relaciones y procesos ~~diseñados y ejecutados para dirigir y controlar~~ para planificar, construir, ejecutar y monitorear la tecnología de la información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.
		Se incluye la definición para atender parte de la observación 74 y otras referenciadas a esta.	e)Gobierno de TI: Subcomponente del gobierno corporativo, el cual, se encarga de la evaluación, dirección y supervisión de las tecnologías de información.
d) ISACA: Acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association).			**fd) ISACA:** Acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association).
e) Marco de gestión de TI: Conjunto de procesos destinados a gestionar las tecnologías de información de las entidades y empresas supervisadas, para la gestión integral de sus riesgos tecnológicos, considerando su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica que estas tienen en los procesos de TI.		Se ajustó la redacción de la definición de "marco de gestión de TI para incluir gobierno.	**ge) 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, ~~para la gestión integral de sus riesgos tecnológicos,~~ 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.
f) 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.			**hf) 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.
g) 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.			**ig) 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.
h) Procesos críticos: Son aquellos procesos que tienen un impacto significativo en la consecución de los objetivos estratégicos previstos por la entidad o			**jh) 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.			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.
i)Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios relacionados con TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).	**[85]COOPEMEP** Valorar la siguiente modificación: Modificar la definición: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios relacionados con TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).Por este texto recomendado: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios de TI críticos a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).Considerando que la definición: Bienes y servicios de TI críticos: Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación.	**[85] No procede** Al incluir en la definición a los proveedores de bienes o servicios críticos que proveen bienes o servicios relacionados con TI, se busca que las entidades y empresas supervisadas a través de su Sistema de Gestión de Seguridad de la Información y de su Marco de Administración Integral de Riesgos atiendan los riesgos que existen en la cadena de proveedores que gestionan la información que está en custodia de las entidades y empresas supervisadas. *****Se ajustó la redacción para mejorar el entendimiento y mantener la congruencia con lo dispuesto en el reglamento.	**ki)Proveedores de bienes y servicios de TI críticos:** Persona física o jurídica que provee bienes o servicios ~~relacionados con~~ de TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).
	[86]COOPEBANPO Modificar la definición: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o	**[86] No procede** Al incluir en la definición a los proveedores de bienes o servicios críticos que proveen bienes o servicios relacionados con TI, se busca que las	

	servicios relacionados con TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).Por este texto recomendado: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios CRITICOS de TI a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).Considerando que la definición: Bienes y servicios de TI críticos: Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación.	entidades y empresas supervisadas a través de su Sistema de Gestión de Seguridad de la Información y de su Marco de Administración Integral de Riesgos atiendan los riesgos que existen en la cadena de proveedores que gestionan la información que está en custodia de las entidades y empresas supervisadas.	
	[87]AAP Se propone como redacción alternativa al inciso i): Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios de TI críticos a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o asociados.	**[87]No procede** Al incluir en la definición a los proveedores de bienes o servicios críticos que proveen bienes o servicios relacionados con TI, se busca que las entidades y empresas supervisadas a través de su Sistema de Gestión de Seguridad de la Información y de su Marco de Administración Integral de Riesgos atiendan los riesgos que existen en la cadena de proveedores que gestionan la información que está en custodia de las entidades y empresas supervisadas.	
	[88]CIS	**[88] No procede**	

	Se sugiere: Modificar la definición: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios relacionados con TI a la entidad o empresas supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).Por este texto recomendado: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios de TI críticos a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).Considerando que la definición: Bienes y servicios de TI críticos: Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos o reputación.	Al incluir en la definición a los proveedores de bienes o servicios críticos que proveen bienes o servicios relacionados con TI, se busca que las entidades y empresas supervisadas a través de su Sistema de Gestión de Seguridad de la Información y de su Marco de Administración Integral de Riesgos atiendan los riesgos que existen en la cadena de proveedores que gestionan la información que está en custodia de las entidades y empresas supervisadas.	
j) 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.			**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.

k) Seguridad cibernética: Práctica de proteger sistemas, redes, dispositivos y datos digitales contra amenazas, ataques y actividades maliciosas en el ciberespacio, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información y de los recursos digitales.	**[89]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.	**[89] Procede** Se agrega la definición de seguridad de la información.	**mk) Seguridad cibernética:** Práctica de proteger sistemas, redes, dispositivos y datos digitales contra amenazas, ataques y actividades maliciosas en el ciberespacio, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información y de los recursos digitales.
	[90]COOPEANDE No se encuentra la definición de seguridad de la información, solo se indica la definición de seguridad cibernética. No son lo mismo, y esto puede provocar confusión a la hora de conocer el alcance y responsabilidades propias de seguridad de la información que no solo vela por el activo digital (TI).	**[90] Procede** Se agrega la definición de seguridad de la información. 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.	
	[91]ISACA Me parece que esta definición está combinando dos definiciones, la de seguridad cibernética y la de seguridad de la información, donde la primera es un subconjunto de la segunda. Definiría Seguridad cibernética como: "Práctica de gestionar los riesgos en los recursos digitales (sistemas, redes, dispositivos y datos) expuestos a amenazas tales como ataques informáticos y actividades maliciosas relacionadas con el ciberespacio, con el objetivo de garantizar una adecuada protección de la seguridad de la información y	**[91] Procede** Procede. Se ajusta la redacción considerando parte de la observación, Adicionalmente, se agrega la definición de seguridad de la información.	

	privacidad de los datos." y definiría Seguridad de la Información como: "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."		
		Se incluye la definición para atender parte de la observación 91 y otras referenciadas a esta.	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.
l)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~~l~~)**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.
m)Unidad de TI o función equivalente: Instancia o función que provee los procesos y servicios de TI para las entidades y empresas supervisadas.			p~~m~~)**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.	**[92]COOPEFYL** Con respecto al anexo 2 de los lineamientos generales, es importante que se armonicen con los establecido en el artículo 3 del presente reglamento ya se exime a las cooperativas de ahorro y	**[92]No procede** 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	Los superintendentes podrán emitir, conjuntamente, los lineamientos generales que consideren necesarios para la aplicación de este reglamento.

	crédito sujetas de regulación proporcional del marco de gobierno y gestión de TI, y luego se incluye vía Lineamientos Generales. Favor aclarar.	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 presente 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 de riesgo, el nivel de tolerancia al riesgo y las políticas aprobadas por el Órgano de Dirección.	**[93]COOPEFYL** Se exime de la aplicación de capítulo a las cooperativas de ahorro y crédito sujetas al Acuerdo Sugef 25-23. Favor revisar los lineamientos generales del anexo 2, ya que están aplicando para efectos de la Auditoría Externa que al menos se tengan procesos de gestión de TI, por tanto, en apariencia hay una contradicción.	**[93]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. 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 presente reglamento**.**	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 nivel de tolerancia al riesgo;~~ el tamaño, complejidad, modelo de negocio y las políticas aprobadas por el Órgano de Dirección.
	[94]COOPEANDE	**[94] No procede**	

	Considerar dejar más claro la responsabilidad de la entidad de definir el alcance de aplicación del Marco de Gobierno y Gestión de TI, es importante dejar esa claridad para evitar interpretaciones por ejemplo por parte de las Auditorías Externas.	Para efectos de la auditoría externa de TI, el "Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI", entre otras disposiciones establece que: 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.	
	[95]FEDEAC Dejar clara la responsabilidad de la entidad de definir el alcance de aplicación del Marco de Gobierno y Gestión de TI, es importante dejar esa claridad para evitar interpretaciones, por ejemplo, por parte de las Auditorías Externas.	**[95] No procede** Para efectos de la auditoría externa de TI, el "Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI", entre otras disposiciones establece que: 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.	
	[96]BAC De acuerdo con lo indicado en la sesión del 13 de diciembre 2023 con los reguladores, se solicita aclarar en el reglamento, que los procesos indicados en el Anexo 1	**[96] No Procede** La propuesta de modificación reglamentaria toma como base diferentes estándares internacionales, mejores prácticas y marcos de referencia; no uno solo en particular.	

	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 acuerdo a su definición y apetito de riesgo, sin que esto signifique necesariamente que está obligada a implementar y evaluar todas las actividades del marco de referencia. En este caso COBIT 2019.	Adicionalmente, en el "Artículo 6 Marco de gobierno y gestión de TI", indica entre otras disposiciones 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 este reglamento. Por otra parte, el "Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI", entre otras disposiciones establece que: 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.	
	[97]COOPEALIANZA Se indica que la entidad debe de diseñar, implementar, controlar y mantener un marco de gobierno, 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 a la entidad diseñar la metodología de acuerdo a su	**[97] 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 destacar, que con la presente propuesta de modificación regulatoria, a su vez, se actualizó la matriz de evaluación, en la	

	estrategia organizacional, el apetito de riesgo, el nivel de tolerancia al riesgo 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 2019donde hasta un nivel 2 es Mejorable, hasta un nivel 3 es Aceptable y por encima de nivel 3 es Fuerte.	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.	
	[98]VIDAPLENA A lo largo de diferentes puntos del Reglamento general de gobierno y gestión de la tecnología de la información, acuerdo CONASSIF 5-24 se hace mención o solo utilizan el apetito y tolerancia, pero no consideran o hacen mención sobre el nivel de capacidad en el momento de establecer los niveles de riesgo.	**[98] Procede** Se realizan los ajustes a la redacción.	
	[99]CFBNCR Respecto al artículo 6, se considera importante que se clarifique en el reglamento si el acuerdo especifica un modelo determinado o si las instituciones pueden analizar, valorar y actualizar su marco en función de	**[99] No procede** El artículo 6 entre otras indica 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	

	los estándares o modelos que se liberan en la industria.	gestión de TI, sin perjuicio del cumplimiento de las disposiciones establecidas en este reglamento, para analizar, valorar y actualizar su marco.	
	[100]ABC Se debe clarificar si el reglamento especifica un modelo determinado o si las instituciones pueden analizar, valorar y actualizar su marco en función de los estándares o modelos utilizados por la industria. El Reglamento genera un desafío importante considerando que no se definen cuáles estándares internacionales son preferibles .Si bien la norma indica que las entidades pueden utilizar los estándares internacionales y las mejores prácticas de la industria de tecnología, los lineamientos generales no parecen dar un margen amplio a las entidades para elegir los estándares de implementación, ya que carecen de la generalidad suficiente, y por el contrario, son exigencias sumamente específicas sobre el modo de dar cumplimiento a la normativa, las cuales podrían no estar alineadas a los estándares o mejores prácticas que finalmente elija seguir la entidad.	**[100] No procede** Las disposiciones establecidas en los lineamientos adjuntos a la presente propuesta regulatoria contienen las pautas relevantes para las superintendencias que buscan homologar los criterios a nivel de todo el sistema financiero costarricense. Las pautas dispuestas en los lineamientos están alineadas a los estándares, mejores prácticas y marcos de referencia internacionales, implementados comúnmente por la industria de las tecnologías de información. Adicionalmente la mayoría de los estándares, mejores prácticas y marcos de referencia internacionales, contienen referencias informativas para conocer el alineamiento de dichos estándares, mejores prácticas y marcos de referencia internacionales con otros. En virtud de lo anterior, las entidades y empresas supervisadas deben validar que los estándares, mejores prácticas y marcos de referencia internacionales, adoptados y adaptados cumplan con las disposiciones de la presente propuesta, y cuando presenten deviaciones definir de forma proactiva los respectivos planes de acción para evitar incumplimientos regulatorios.	
	[101]BCR Pregunta • Dado que se tiene que incorporar 6 procesos adicionales, ¿esta modificación de su alcance se debe de comunicar a las	**[101]No procede** Se atiende como consulta. Respuesta; Las entidades y empresas supervisadas deben comunicar a las superintendencias	

	Superintendencias?, ¿de qué forma y cuándo? • Se debería aclarar qué es gobierno corporativo, gobierno de TI y gestión de TI. Nuestra recomendación va en sentido de que quede bien claro los diferentes tipos de gobernanza, y de gestión, para comprender las responsabilidades y ámbito de acción según cada concepto. • Separando el gobierno y la gestión de la Unidad de TI desde la información y tecnología (I&T).	a través del perfil tecnológico los procesos de evaluación aplicables a su marco de gobierno y gestión de TI, de conformidad con lo establecido en el "Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI" 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, adicionalmente, se incluyó la definición de marco de gobierno y gestión de TI.	
	[102]ACOP En relación con esta norma, es muy importante que en forma expresa se limite la competencia de la Supen, en relación con la potestad de modificar el marco de gobierno y gestión de TI, así como de establecer e imponer estándares internacionales o mejores prácticas de la industria de TI; respetándose así la autodeterminación de la Operadora.	**[102] No procede** El "Articulo 6 Marco de Gobierno y Gestión", indica que son las entidades y empresas supervisadas las que deben diseñar, implementar, controlar y mantener su marco de gobierno y gestión de TI de conformidad con la estrategia organizacional, el apetito, la tolerancia y la capacidad de riesgo, así como las políticas aprobadas por el Órgano de Dirección. Asimismo, las entidades y empresas supervisadas podrán utilizar los estándares internacionales, mejores prácticas y marcos de referencia que la industria de tecnologías ha desarrollado para la implementación del marco de gobierno y gestión de TI, sin perjuicio del cumplimiento de las disposiciones establecidas en este reglamento. Por su parte, el "Artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI", indica entre otras disposiciones 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 perjuicio de lo anterior, mediante acto administrativo, las Superintendencias podrán ampliar la cantidad de procesos de evaluación declarados en el perfil tecnológico de acuerdo con las necesidades de supervisión, el riesgo identificado o cuando se determine que el marco de gobierno y gestión de TI no es acorde con las particularidades de las entidades o empresas supervisadas.	
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.			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.
		Se incluye un párrafo para ampliar sobre el tema de implementación del marco de gobierno y gestión de TI.	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:	**[103]BNCR Pregunta** ¿Cuál es el plazo que se tiene para implementar el proceso de aseguramiento?	**[103]No procede** Se atiende como consulta. Respuesta Las entidades y empresas supervisadas deben validar que cumplan con las disposiciones del presente reglamento, y cuando presenten brechas definir de forma proactiva los respectivos planes	El marco de gobierno y gestión de TI debe permitir a las entidades y empresas supervisadas cumplir con los siguientes propósitos:

		de implementación para atender de manera oportuna dichas brechas. Por otra parte, se incluyó una disposición transitoria para la implementación de dichas brechas identificadas. Las entidades dispondrán de un plazo no mayor a tres años para finalizar los planes de implementación, lo anterior, sin perjuicio del cumplimiento de los demás plazos establecidos en este reglamento.	
	[104]BPDC Se sugiere incluir "Asegurar el cumplimiento normativo y de la legislación nacional aplicable"	**[104] Procede** Se incorpora parte de las observaciones para aclarar el texto.	
	[105]MUCAP 1) No existe claridad cuales indicadores de cumplimiento se estarán utilizando para medir el cumplimiento de estos propósitos. Adicionalmente, existe la incertidumbre sobre los marcos de referencia que se estarían utilizando en las Auditorías Externas, para evaluar a la entidad. 2) No que queda claro si la función de TI puede ser llevada a cabo por varias unidades de TI en la entidad. 3) No existe claridad sobre el concepto "incidentes de los bienes y servicios".	**[105]Procede** Se ajusta la redacción para aclarar que es una unidad de TI, no varias y para mejorar la claridad en relación con la observación de "incidentes de los bienes y servicios" Por otra parte, 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.	
	[106]COOPEANDE Valorar incluir dentro de los propósitos del Marco de Gobierno y Gestión de TI, que la gestión de la tecnología sea transversal en la entidad y no una responsabilidad única de las áreas de tecnología.	**[106] Procede** Se ajusta la redacción del artículo 6 para incorporar parte de lo indicado en esta observación	
	[107]FEDEAC	**[107]Procede**	

	Valorar incluir dentro de los propósitos del Marco de Gobierno y Gestión de TI, que la gestión de la tecnología sea transversal en la entidad y no una responsabilidad única de las áreas de tecnología. La periodicidad de cambios, planificación y desarrollo de TI debe ir alineada con los cambios estratégicos de la entidad y cambios normativos.	Se ajusta la redacción del artículo 6 para incorporar parte de lo indicado en esta observación	
	[108]COOPESERVIDORES 1. Aclarar para el punto d) si se refiere a planificación operativa, estratégica, de recursos humanos, financieros o qué tipo de planificación relacionada a las tecnologías de información se refiere? Porque tiende a confundir que los puntos e y f que también indican el tema de estrategia. 2. Aclarar en el lineamiento h) si está pidiendo acuerdos de nivel de servicio para los riesgos de TI? No queda clara esta combinación si es que está solicitando una gestión de acuerdo de nivel de servicio para los riesgos de TI, y si es correcta esta interpretación? o más bien lo que quiere dar entender es que se deben gestionar los riesgos de TI para los proveedores de bienes y servicios de TI ?De igual forma no concuerda esta parte "Además del diseño e implementación de sistemas integrados de calidad y de seguridad de la información, así como la gestión de activos de información y de los datos." con la gestión de acuerdos de niveles de servicio, se interpreta como una	**[108]Procede** Se ajusta redacción para aclarar los propósitos del marco de gobierno y gestión de TI.	

	mezcla de varios temas, pero entre ambos no tienen concordancia.		
	[109]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.	**[109]Procede** Se ajusta la redacción para mejorar el entendimiento de las disposiciones.	
	[110]CFBNCR Referente a los artículos 6 y 7, se considera que en la actualidad el aseguramiento es una función transversal a nivel del ciclo de TI, es decir, se ejecuta de manera integral en procesos clave tales como identificación y construcción de soluciones, gestión de cambio, aceptación del cambio y transición. En este contexto, se considera importante conocer el alcance de los controles y el plazo de implementación que la norma en consulta estaría estableciendo para este proceso, de manera que sea posible identificar eventuales brechas en los procesos, así como priorizar las acciones que permitan gestionar el debido cumplimiento en tiempo y forma. Sobre el inciso f, se sugiere modificar este propósito de la siguiente manera: “Utilizar	**[110] Procede** 1-Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias. 2-Respecto al punto 2, se aclara que el texto de los incisos f y l fue modificada, pero con una redacción distinta a la sugerida.	

	herramientas como la planificación estratégica, la gestión de la innovación y la arquitectura organizacional, como elementos de apoyo a la gestión organizacional". Sobre el inciso l, 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".		
	[111]ABC En la actualidad el aseguramiento es una función transversal a nivel del ciclo de TI, es decir, se ejecuta de manera integral en procesos clave, tales como identificación y construcción de soluciones, gestión y aceptación de cambio y transición. Por ello, es necesario conocer el alcance de los controles y el plazo de implementación que la norma en consulta estaría estableciendo para este proceso, para efectos de identificar eventuales brechas y priorizar las acciones que permitan gestionar el debido cumplimiento.	**[111] Procede** Para las brechas que se identifiquen se incluyó una disposición transitoria.	
	[112]CB Inciso f:Comentarios:Sobre el inciso f, se sugiere modificar este propósito de la siguiente manera: "Utilizar herramientas como la planificación estratégica, la gestión de la innovación y la arquitectura organizacional, como elementos de apoyo a la gestión organizacional" .Inciso	**[112]Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	

	l:Comentarios:Sobre el inciso l, 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”.		
	[113]ISACA No se hace la distinción y relación entre la continuidad de TI y la del Negocio. No se identifican lineamientos relacionados con la Continuidad del Negocio, se menciona la resiliencia digital, así como el tema de cibernética, pero mientras la Banca continue siendo presencial, la TIC se deberá recuperar de forma integral con las operaciones del negocio, todo aquello que no es información estructurada.	**[113] No procede** Las entidades y empresas supervisadas podrían optar de forma complementaria por la adopción de mejores prácticas, estándares internacionales, y marcos de referencia internacional de forma complementaria para perfeccionar sus sistemas de control interno. Las entidades y empresas supervisadas para el diseño e implementación de los estándares, mejores prácticas y marcos de referencia deben considerar su adaptación para la consecución de los objetivos organizaciones y la atención de los riesgos. Por ejemplo, estándares como la ISO 22301 definen que se debe establecer planes de continuidad, por lo que las entidades y empresas supervisadas pueden desarrollar planes de continuidad generales o específicos, lo anterior con el fin de responder a incidentes disruptivos y cómo continuará o recuperará sus actividades, estos planes pueden variar según el modelo, tamaño y complejidad del negocio. Por su parte, estándares como la ISO 22301 para aspectos relacionados con la recuperación, definen que se debe establecer procedimientos	

		documentados para restaurar y retornar a las actividades del negocio desde las medidas adoptadas temporalmente para soportar los requisitos normales del negocio después de un incidente. La resiliencia operativa es la capacidad de una organización para resistir una disrupción repentina y recuperarse. Antes, ese concepto era sinónimo de continuidad del negocio o recuperación de desastres. Pero gracias a la digitalización de los negocios, la resiliencia operativa se convirtió en algo más profundo: una mezcla de continuidad del negocio, gestión de riesgos de proveedores, ciberseguridad y más. Considerando lo anterior, las entidades y empresas supervisadas son las responsables de establecer los mecanismos de control de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos.	
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.			b) Asegurar un equilibrio entre el uso de los recursos de TI y los procesos críticos de negocio.
c)Crear valor mediante los beneficios de las tecnologías de información, dentro de los márgenes de apetito al riesgo.			c)Crear valor mediante los beneficios de las tecnologías de información, dentro de los márgenes de apetito, tolerancia y capacidad de ~~al~~ riesgo.
d)Asegurar que la planificación y el desarrollo de TI se realice de conformidad con lo definido por la entidad o empresa supervisada, de tal forma que se garantice que TI contribuye en satisfacer las necesidades y expectativas organizacionales.		Se modifica la redacción con base en lo indicado en las observaciones.	~~d)Asegurar que la planificación y el desarrollo de TI se realice de conformidad con lo definido por la entidad o empresa supervisada, de tal forma que se garantice que TI contribuye en satisfacer las necesidades y expectativas organizacionales.~~ d)Asegurar que la entidad o empresa supervisada dispone de recursos adecuados y suficientes para el gobierno y la gestión de TI.

e)Establecer una dirección estratégica sólida y una estructura eficiente para gestionar TI; asimismo, alinear los objetivos de la entidad o empresa supervisada con el uso de la tecnología y su arquitectura organizacional.		Se modifica la redacción con base en lo indicado en las observaciones.	~~e)Establecer una dirección estratégica sólida y una estructura eficiente para gestionar TI; asimismo, alinear los objetivos de la entidad o empresa supervisada con el uso de la tecnología y su arquitectura organizacional.~~ e)Asegurar que se identifica e involucra a las partes interesadas en el diseño del marco de gobierno y gestión de TI.
f) Implementar la planificación estratégica, así como la gestión de la innovación y de la arquitectura organizacional.		Se modifica la redacción con base en lo indicado en las observaciones.	~~f) Implementar la planificación estratégica, así como la gestión de la innovación y de la arquitectura organizacional.~~ f)Diseñar e implementar el marco de gobierno y gestión de TI de conformidad con los objetivos y riesgos del negocio.
g) Gestionar el presupuesto, los costos, el conocimiento y el recurso humano de las unidades de TI, así como las relaciones con las partes interesadas.		Se modifica la redacción con base en lo indicado en las observaciones.	~~g) Gestionar el presupuesto, los costos, el conocimiento y el recurso humano de las unidades de TI, así como las relaciones con las partes interesadas.~~ 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 la gestión de los acuerdos de nivel de servicio, de los proveedores de bienes y servicios de TI y de los riesgos de TI. Además del diseño e implementación de sistemas integrados de calidad y de seguridad de la información, así como la gestión de activos de información y de los datos.	**[114]CAJAANDE** H. Respetuosamente les solicitamos aclarar a qué se refieren con gestión de datos.	**[114]No procede** Se atiende como consulta. Respuesta: Gestionar los datos es la gestión eficaz de los activos de datos de la organización durante todo el ciclo de vida de los datos, desde la creación hasta su entrega, mantenimiento y archivo, con el fin de lograr el uso eficaz de activos de datos críticos y la consecución de los objetivos de la entidad o empresa supervisada. Además, se modifica la redacción con base en lo indicado en las observaciones.	~~h) Establecer la gestión de los acuerdos de nivel de servicio, de los proveedores de bienes y servicios de TI y de los riesgos de TI. Además del diseño e implementación de sistemas integrados de calidad y de seguridad de la información, así como la gestión de activos de información y de los datos.~~ 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)Definir la gestión del portafolio y de los programas y proyectos de TI que permitan atender la definición de los requisitos del negocio, según corresponda.		Se modifica la redacción con base en lo indicado en las observaciones.	~~i)Definir la gestión del portafolio y de los programas y proyectos de TI que permitan atender la definición de los requisitos del negocio, según corresponda.~~

			i)Gestionar la innovación, las tecnologías emergentes, el conocimiento y los datos relacionados con la entidad o empresa supervisada.
j) Determinar la estrategia de adquisición, construcción e implementación de soluciones tecnológicas integradas al negocio.		Se modifica la redacción con base en lo indicado en las observaciones.	~~j) Determinar la estrategia de adquisición, construcción e implementación de soluciones tecnológicas integradas al negocio.~~ 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) Gestionar la disponibilidad y la capacidad de infraestructura tecnológica y asegurar la continuidad de las operaciones.		Se modifica la redacción con base en lo indicado en las observaciones.	~~k) Gestionar la disponibilidad y la capacidad de infraestructura tecnológica y asegurar la continuidad de las operaciones.~~ 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)Asegurar la configuración de los activos de información, considerando la gestión, aceptación y transición de los cambios.		Se modifica la redacción con base en lo indicado en las observaciones.	~~l)Asegurar la configuración de los activos de información, considerando la gestión, aceptación y transición de los cambios.~~ 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)Gestionar las operaciones de TI, los incidentes de los bienes y servicios, además, la solución de los problemas de TI, los servicios de seguridad de la información y de seguridad cibernética, los controles de los procesos del negocio, así como asegurar una resiliencia operativa digital.		Se modifica la redacción con base en lo indicado en las observaciones.	~~m)Gestionar las operaciones de TI, los incidentes de los bienes y servicios, además, la solución de los problemas de TI, los servicios de seguridad de la información y de seguridad cibernética, los controles de los procesos del negocio, así como asegurar una resiliencia operativa digital.~~ 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) Gestionar el monitoreo del desempeño y la conformidad de los procesos, el sistema de control interno, el cumplimiento de los requisitos externos y el aseguramiento de TI.		Se modifica la redacción con base en lo indicado en las observaciones.	~~n) Gestionar el monitoreo del desempeño y la conformidad de los procesos, el sistema de control interno, el cumplimiento de los requisitos externos y el aseguramiento de TI.~~ n)Determinar la estrategia de adquisición, construcción e implementación de soluciones tecnológicas integradas al negocio.

		Se incorpora texto con base en lo indicado en las observaciones.	o)Gestionar la disponibilidad y la capacidad de infraestructura tecnológica, así como asegurar la continuidad de las operaciones.
		Se incorpora texto con base en lo indicado en las observaciones.	p)Asegurar la configuración de los activos de información de conformidad con la gestión, aceptación y transición de los cambios.
		Se incorpora texto con base en lo indicado en las observaciones.	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.
		Se incorpora texto con base en lo indicado en las observaciones.	r)Gestionar el monitoreo del desempeño y la conformidad de los procesos, el sistema de control interno, el cumplimiento de los requisitos externos, así como el cumplimiento normativo, la legislación nacional aplicable, y el aseguramiento de TI.
		Se incorpora texto con base en lo indicado en las observaciones.	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:	**[115]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."	**[115] 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:
	[116]MUCAP 1) No existe claridad si al definir "apetito de sus riesgos asociados", implica que el marco de gobierno y gestión de TI debe tener sus riesgos, siendo estos los que identifica el Auditor Externo o los	**[116]Procede** Los puntos 2 y 5 proceden y se ajusta la redacción considerando lo sugerido. Para los demás puntos se incluye a continuación el motivo por el cual no se consideran como posibles ajustes dentro de la disposición.	

	identificados a nivel interno, por ende, surge la duda si las entidades deberían establecer un proceso de identificación de riesgos sobre el marco de gobierno y gestión de TI. 2) No existe claridad sobre la función específica debe ejecutar el Órgano de Dirección, respecto a las tecnologías emergentes. 3) Como está indicado este inciso, faculta la interpretación de que la competencia del Órgano de Dirección es establecer las políticas generales para asegurar que se resguarde lo ahí indicado. Nuevamente, se hace la observación con respecto al adjetivo "crítico" Ver comentario al artículo 4 inciso i). 4)Adicionalmente, no existe claridad si esta responsabilidad aplica solo para la información que es utilizada por los proveedores de la entidad supervisada y no para la información que gestionada en la entidad. 5)Además, Como está redactado surge la duda si el Órgano de Dirección es quien debe asegurar que la información usada por los proveedores es resguardada. Bajo este sentido, las implicaciones que tendría la palabra asegurar, no quedan claras, ya que esa es una función de gestión y no de gobierno; es decir, lo que hace denotar que se la está dando a la Junta Directiva una función de gestión.	1)El análisis de los riesgos del marco de gobierno y gestión de TI y cualquier otro riesgo, forman parte del proceso de gestión de riesgos que defina las entidades o empresas supervisadas. 2) Se ajusta la redacción para mejorar el entendimiento del texto en relación con la observación de que "No existe claridad sobre la función específica debe ejecutar el Órgano de Dirección, respecto a las tecnologías emergentes". 3)El concepto de impacto significativos debe ser asignado por cada entidad de conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos. 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 internacionales y marcos de referencia aplicables a la industria de las TI. En todo caso deben estar documentas a nivel de la organización todas las políticas, procedimientos, instructivos y formularios que permitan sistematizar y repetir dichos análisis como parte de sus procesos de negocio. Por su parte las entidades y empresas supervisadas son las responsables de establecer los mecanismos dentro de sus planes alternos de trabajo para atender posibles situaciones contingentes, en este sentido, dichos mecanismos de control deberán estar diseñados, implementados y probados de	

		conformidad con el tamaño, complejidad, modelo de negocio y riesgos asociados a sus procesos, bienes o servicios dentro del sector en el que opera y brinda estos. 5) Se ajusta la redacción para mejorar el entendimiento del texto y se mueve la responsabilidad para la Alta Gerencia. Tanto el Reglamento de Gobierno Corporativo CONASSIF 4-16, y el marco de referencia CobiT, utilizan el infinitivo "Asegurar", para denotar responsabilidades de gobierno. Las entidades y empresas supervisadas deberán establecer a su vez las estructuras, funciones y mediadas que permitan implementar o gestionar dichas expectativas de alto nivel, dentro de sus procesos operativos.	
	[117]CFBNCR 1-Para los artículos 8,9,10,11,13,14 y 15 Se sugiere revisar la pertinencia de algunas responsabilidades establecidas en las secciones II, III y IV, dada la existencia del principio de proporcionalidad. Enel entendido que, en apego a las facultades definidas por ley, el órgano de dirección tiene funciones asociadas principalmente a la aprobación de políticas, el apetito de riesgo, reglamentos, la estrategia de la entidad, asignar responsabilidades y recursos, entre otros y es responsabilidad de la administración activa su ejecución, además de alinear los procesos, procedimientos, registros a los criterios aprobados por el órgano.	**[117]No procede** 1-Las responsabilidades establecidas en la presente modificación reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta. 2-Algunas de las responsabilidades fueron ajustadas con los infinitivos correspondientes al órgano de dirección. 3-El capítulo II Gobierno y Gestión de TI contiene las expectativas de alto nivel esperadas por las Superintendencias, las cuales están separadas en los aspectos más relevantes que se espera que las entidades y empresas supervisadas deban atender con el fin de mitigar posibles riesgos y su impacto en el Sistema Financiero Nacional. 4-Las responsabilidades contenidas en la presente modificación reglamentaria complementan y refuerzan los	

	Dicho lo anterior, se considera que algunas funciones están utilizando verbos descritos en términos de funciones administrativas y operativas que son más bien responsabilidad del Administración, y no del órgano de dirección ni de los comités de apoyo. Por ejemplo, no es competencia del órgano de dirección el aplicar una evaluación, pero sí debe velar porque se establezca, supervisar y conocer los resultados de la evaluación y dimensionar los alcances. En ese sentido, se sugiere una revisión integral de los alcances consignados en esas secciones, para una adecuada asignación de responsabilidades, conforme al rol de cada una de las partes y las mejores prácticas. 3-Para efectos de facilitar la aplicación del acuerdo en cuestión, se recomienda que los lineamientos de la gestión de los procesos sobre la seguridad de la información y la seguridad cibernética, evaluación de las necesidades de las partes interesadas y la estrategia para la resiliencia operativa digital estén contenidas en el marco de gobierno y gestión de TI, donde se delimiten las responsabilidades de las partes involucradas en su ejecución. Aplicando esta recomendación, podría generarse un único artículo de responsabilidades que se homologuen o alineen en	mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta y adicionalmente las establecidas en el reglamento CONASSIF 4-16.	

	estructura y alcance a otros reglamentos vigentes como: CONASSIF 4-16, CONASSIF 12-21 y SUGEF 2-10. 4-Respecto a la gestión del comité de TI, también le aplica el principio de proporcionalidad por lo que se sugiere alinear su gestión al artículo 24 del acuerdo CONASSIF 4-16 Reglamento de Gobierno Corporativo y no concentrar sus funciones en aspectos administrativos que son responsabilidad de la Administración, pero sí es responsabilidad de la Administración el rendir cuentas de la gestión de aplicación del marco de gobierno y gestión de TI que incluyan aspectos como resultados de evaluaciones al proceso, ya sean internas o externas, implementación de la estrategia, indicadores de desempeño, entre otros.		
	[118]CB Comentarios: Se solicita revisar con detalle las responsabilidades establecidas en las secciones II, III y IV del Capítulo II sobre Gobierno y Gestión de TI, debido a que se considera que muchos son temas administrativos y operativos y se está asignando sin considerar el principio de proporcionalidad. Para citar solo un ejemplo: en el inciso h) se establece que el Órgano de Dirección debe "asegurar" que la información usada por los proveedores es resguardada. Esa es una función de	**[118] Procede** Se atiende como parte de la consulta [117], y adicionalmente se traslada la responsabilidad del inciso "h" como parte de las responsabilidades de la Alta Gerencia, ajustando su redacción.	

	gestión y no de gobierno, con lo cual se está asignando a la Junta una función de gestión. Inciso h: Comentarios: Surge la duda si el Órgano de Dirección es quien debe asegurar que la información usada por los proveedores sea resguardada. Se considera que esa es una función de gestión y no de gobierno; es decir, que se le está asignando a la Junta Directiva una función operativa de gestión. En tal sentido, más bien se debería incluir un inciso que establezca 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.		
	[119]BCR • Se amplían y se adicionan más funciones al Órgano de Dirección, sin embargo, notamos que no se amplían las funciones del Comité de TI con respecto a las nuevas funciones del órgano de dirección. Nuestra recomendación sería, que, si se incluyen funciones al órgano de dirección, también deberían incluirse al Comité de TI para que este le dé apoyo al órgano de dirección en dichos temas.	**[119]No procede** De conformidad con el Acuerdo CONASSIF 4-16 "Reglamento de Gobierno Corporativo", para lograr la eficiencia y una mayor profundidad en el análisis de los temas de su competencia, el Órgano de Dirección debe establecer comités técnicos. Dichos comités deben contar con una normativa, que regule su funcionamiento, integración, el alcance de sus funciones, y los procedimientos de trabajo, esto incluye la forma en que informará al Órgano de Dirección.	
	[120]CCPA Observando documentos como los principios de Gobierno Corporativo de la OCDE, mejores prácticas Gobierno Corporativo del IGC, las funciones de este tipo de organismos se orientan a	**[120] No procede** Se traslada la responsabilidad del inciso "h" como parte de las responsabilidades de la Alta Gerencia, ajustando su redacción.	

	garantizar la orientación estratégica de la empresa, la implementación de controles y la rendición de cuentas, de aquí que en el inciso h se describe mejor utilizar el término supervisar, implementar, verificar que Asegurar. Se sugiere agregar un inciso donde se indique "y cualquier otra responsabilidad que este dentro del alcance del órgano de dirección".		
a) Aprobar el marco de gobierno y gestión de TI y el apetito de sus riesgos asociados.	**[121]BNCR** Relacionado con el apartado "a", actualmente en el BNCR lo que se lleva a aprobación por parte de la Junta Directiva es el Reglamento del Comité de TI ¿Esto sería suficiente o se requiere que la Junta Directiva también apruebe el Marco de Gobierno de TI?	**[121] No procede** En el Acuerdo CONASSIF 5-17, y sus lineamientos, se indica que el marco de gestión de TI debe ser aprobado por el Órgano de Dirección, por otra parte, la propuesta reglamentaria se mantiene dicha disposición, adicionalmente en la propuesta se incluye que se debe aprobar el apetito de sus riesgos asociados, como parte de la declaración de apetito de riesgo de la organización, adicionalmente se ajusta la redacción para mejorar el entendimiento. *****Por otra parte, se modifica el texto para mejorar el entendimiento de la disposición.	a) Aprobar el marco de gobierno y gestión de TI, así como asegurar que la declaración de ~~y el~~ apetito de ~~sus~~ riesgos incorpore el apetito, la tolerancia y la capacidad de los riesgos asociados a TI.
	[122]COOPEANDE Aprobar el marco de gobierno y gestión de TI y el apetito de sus riesgos asociados, en esta responsabilidad del Órgano de Dirección, especificar la aprobación del alcance del marco de gobierno y gestión de TI.	**[122]No procede** El "Artículo 43 Procesos de evaluación del marco de gobierno y gestión de TI", indican entre otras aspectos que las entidades y empresas supervisadas deben indicar en el perfil tecnológico cuáles de los procesos de evaluación detallados en los lineamientos generales del presente reglamento resultan adecuados a su marco de gobierno y gestión de TI. Asimismo, las entidades y empresas supervisadas deberán indicar,	

		en el perfil tecnológico, los procesos de evaluación que no les apliquen, así como los que estén externalizados de forma total o parcial. Los procesos de evaluación que no les apliquen deben estar debidamente fundamentados en un estudio técnico, el cual debe ser remitido mediante los canales oficiales de comunicación de cada Superintendencia. Los aspectos que deben ser considerados para la elaboración del estudio técnico están establecidos en los lineamientos generales del presente reglamento.	
	[123]FEDEAC a): Aprobar el marco de gobierno y gestión de TI y el apetito de sus riesgos asociados, en esta responsabilidad del Órgano de Dirección, especificar la aprobación del alcance del marco de gobierno y gestión de TI.	**[123]No procede** El "Artículo 43 Procesos de evaluación del marco de gobierno y gestión de TI", indican entre otras aspectos que las entidades y empresas supervisadas deben indicar en el perfil tecnológico cuáles de los procesos de evaluación detallados en los lineamientos generales del presente reglamento resultan adecuados a su marco de gobierno y gestión de TI. Asimismo, las entidades y empresas supervisadas deberán indicar, en el perfil tecnológico, los procesos de evaluación que no les apliquen, así como los que estén externalizados de forma total o parcial. Los procesos de evaluación que no les apliquen deben estar debidamente fundamentados en un estudio técnico, el cual debe ser remitido mediante los canales oficiales de comunicación de cada Superintendencia. Los aspectos que deben ser considerados para la elaboración del estudio técnico están establecidos en los lineamientos generales del presente reglamento.	

b) Establecer un Comité de TI o una función equivalente y aprobar sus normas de gobierno y gestión.			b) Establecer un Comité de TI o una función equivalente y aprobar sus normas de gobierno y gestión.
c)Designar la firma de auditoría externa o el profesional independiente de TI que realizará las auditorías solicitadas por las Superintendencias.	**[124]ISACA** Relacionado con: "c) Designar la firma de auditoría externa o el profesional independiente de TI que realizará las auditorías solicitadas por las Superintendencias." El Órgano de Dirección sería juez y parte. Precisamente una de las obligaciones de este ente debería ser participar en la auditoría, es decir el ente es parte de la nómina de auditados, por lo tanto, no debería seleccionar la entidad externa. El Órgano de Dirección no debería aprobar los informes de auditoría externa de TI, o posiblemente es la palabra la incorrecta, debería ser acreditar, refrendar, etc. porque el Órgano de Dirección no debería aprobar un informe realizado de forma independiente.	**[124] No procede** Se eliminó la disposición porque esto ya está establecido en el artículo 4 del Acuerdo CONASSIF 1-10.	~~c)Designar la firma de auditoría externa o el profesional independiente de TI que realizará las auditorías solicitadas por las Superintendencias.~~
d)Aprobar las políticas, estructuras, planes estratégicos, recursos, inversiones y presupuestos necesarios para la implementación del marco de gobierno y gestión de TI, incluyendo tecnologías emergentes.	**[125]POPULARPENSIONES** Se debe de delimitar el alcance de "tecnologías emergentes", actualizar dicho alcance en forma anual, la no delimitación favorece interpretaciones ambiguas.	**[125] No procede** Dentro de las disposiciones reglamentarias no se delimita el alcance o periodicidad sobre tecnologías emergentes, ya que el propósito de la disposición es distinto a lo indicado en la observación. Se mejora la redacción del inciso d).	~~d~~c) Aprobar las políticas, estructuras, ~~planes~~ estrategias ~~égicos~~ recursos, inversiones y presupuestos necesarios para la implementación del marco de gobierno y gestión de TI, ~~incluyendo~~ así como para las tecnologías emergentes que se implementen.
e) Aprobar los informes de la auditoría externa de TI que serán remitidos a las Superintendencias.			d~~e~~) Aprobar los informes de la auditoría externa de TI que serán remitidos a las Superintendencias.
f) 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~~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.
g) Evaluar las necesidades de las partes interesadas para lograr un equilibrio entre los objetivos del	**[126]CATHAY**	**[126] Procede**	~~gf~~) ~~Evaluar~~ Asegurar que se consideren las necesidades de las partes interesadas para lograr un

negocio y los objetivos de TI definidos por la entidad o empresa supervisada.	"Evaluar las necesidades de partes interesadas" es una función muy operativa para ser asumida por un órgano de dirección. Se sugiere reemplazar "Evaluarlas necesidades" por "Supervisar la identificación, integración, monitoreo y evaluación continua de las partes interesadas y sus necesidades para lograr un equilibrio entre los objetivos del negocio y los objetivos de TI definidos por la entidad o empresa supervisada" "Asegurar que se resguarde" es una función o responsabilidad con características muy operativas para un órgano de dirección. Se sugiere: "Asegurar el establecimiento y cumplimiento de políticas y normativas para resguardar la confidencialidad e integridad de los datos y de la información crítica de partes interesadas y de la entidad que sea utilizada por proveedores".	Se ajusta la redacción considerando parte de lo sugerido para aclarar las disposiciones, y se considera lo indicado en las observaciones [117 y 118]	equilibrio entre los objetivos del negocio y los objetivos de TI definidos por la entidad o empresa supervisada.
h) Asegurar que se resguarde la confidencialidad e integridad de los datos y de la información crítica de las partes interesadas y de la entidad o empresa supervisada que sea utilizada por los proveedores.	**[127]Luis Diego León Barquero** Yo cambiaría el punto h) "Asegurar que se resguarde la confidencialidad e integridad de los datos y de la información crítica de las partes interesadas y de la entidad o empresa supervisada que sea utilizada por los proveedores", pues los miembros de la Junta Directiva no tienen el tiempo, conocimiento, experiencia, entre otras competencias para realizar actividades de la administración. De acuerdo con las buenas prácticas de Gobierno	**[127] Procede** Se considera parte de los comentarios para modificar la disposición y se consideran los comentarios en las observaciones [117,118,126]	~~h) Asegurar que se resguarde la confidencialidad e integridad de los datos y de la información crítica de las partes interesadas y de la entidad o empresa supervisada que sea utilizada por los proveedores.~~ g) Designar las áreas de negocio y de TI responsables de diseñar e implementar el marco de gobierno y de gestión TI.

	Corporativo, sobre las responsabilidades principales de la Junta Directiva (estrategia, riesgos y cumplimiento), yo lo redactaría de la siguiente manera: h. Supervisar la implementación de controles para asegurar que se resguarde la confidencialidad e integridad de los datos y de la información crítica de las partes interesadas y de la entidad o empresa supervisada que sea utilizada por los proveedores.		
	[128]COOPEALIANZA Se solicita que el inciso "h", sea integrado en el artículo 9	**[128] Procede** Se ajusta con parte de las recomendaciones, se traslada a las responsabilidades de la Alta Gerencia, y se ajusta la redacción para mejorar el entendimiento de la disposición.	
	[129]ISACA Replantearía este objetivo como "Asegurar que se resguarde la seguridad de la información para garantizar una adecuada protección y privacidad de los datos de partes interesadas y de la entidad o empresa supervisada que sea utilizada por terceras partes dentro de toda la cadena de suministro."	**[129] Procede** Se ajusta con parte de las recomendaciones, se traslada a las responsabilidades de la Alta Gerencia, y se ajusta la redacción para mejorar el entendimiento de la disposición.	
Artículo 9. Responsabilidades sobre la seguridad de la información y la seguridad cibernética	**[130]Luis Diego León Barquero** Se utiliza la palabra asegurar, pero esto puede crear confusión con respecto a los encargos de aseguramiento que hacen los auditores. Adicionalmente, asegurar no es una responsabilidad del órgano de gobierno. De acuerdo con las buenas prácticas de Gobierno Corporativo, sobre las responsabilidades principales	**[130] No procede** Tanto el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, y marcos de referencia internacionales como el caso de CobiT, utilizan el infinitivo "Asegurar" para denotar responsabilidades de gobierno.	**Artículo 9. Responsabilidades sobre la seguridad de la información y la seguridad cibernética**

	de la Junta Directiva (estrategia, riesgos y cumplimiento), yo lo redactaría de la siguiente manera: En relación con el gobierno de la seguridad de la información y de la seguridad cibernética, el Órgano de Dirección, al menos, debe: a) Verificar 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) Asignar tiempo a las discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética en las reuniones del Órgano de Dirección. c) Verificar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles. d) Verificar que se apliquen medidas para la atención de los incidentes de seguridad de la información y de seguridad cibernética. e) Aprobar los planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética. f) Verificar que los requerimientos de seguridad de la información y de seguridad cibernética de la entidad o empresa supervisada sean de cumplimiento por parte de los proveedores de bienes y servicios de TI. Las palabras subrayadas son los cambios propuestos. Puede ser que algunas de estas responsabilidades sean de la Administración.		

	[131]BPDC Pregunta Para el punto (a) se debe confirmar si el Sistema de Gestión de Seguridad de la Información debe ser certificado o no Para el punto (d) se considera que es una función de gestión de muy bajo nivel para ser asignada a un órgano de gobernanza. ¿Debería más bien asegurarse de que se han atendido los incidentes de seguridad y no ver este nivel de detalle? Para el punto (f) una función de gestión de muy bajo nivel para ser asignada a un órgano de gobernanza. ¿Debería más bien asegurarse de que se han atendido los incidentes de seguridad y no ver este nivel de detalle?	**[131]No procede** En ningún caso el marco de regulación hace referencia que la entidad deba certificarse o deba certificar algún proceso de TI. En relación con lo señalado sobre el punto d) de la observación, se trasladan y ajustan las responsabilidades al Artículo 11 Responsabilidades de la Alta Gerencia.	
	[132]MUCAP 1)No existe claridad si estas responsabilidades pueden ser delegadas al Comité de Tecnología de Información. 2) Como está indicado no existe claridad si el tiempo puede ser asignado a criterio de la entidad. No quedando claro si las superintendencias pueden realizar observaciones donde hagan mención que el tiempo determinado no es suficiente. 3) Se considera que la aplicación de medidas para la atención de incidentes es un tema operativo y de gestión, por tal motivo surge la inquietud si con este inciso se pretende que el Órgano de Dirección cumpla esta función.	**[132]Procede** 1-Las responsabilidades indicadas en la sección II, del capítulo II, son responsabilidades del Órgano de Dirección. 2-Se ajusta el texto considerando el comentario de la observación 3-Se atiende como parte de la observación [131 -a] y [131 –“d” y “f”] 4-En el comentario no se indica a cuál documento específico se está haciendo referencia la observación. 5-Se atiende como parte de la observación [131 -a] y [131 –“d” y “f”	

	4) No existe claridad si la superintendencia lo que espera tener es un documento específico para este tema, el cual sea de aprobación del Órgano de Dirección. Lo anterior debido a que en la actualidad es de aprobación del Comité que cumple las funciones del Comité de Seguridad. 5) Se considera que la aplicación de medidas para la atención de incidentes es un tema operativo y de gestión, por tal motivo surge la inquietud si con este inciso se pretende que el Órgano de Dirección cumpla esta función. Como complemento se puede mencionar que se deja a interpretación que cuando se hace referencia a "Asegurar" por parte del Órgano de Dirección, es en el cumplimiento de aprobar la normativa que se sustente a ese alcance, ya que como se indicó no es un órgano operativo.		
	[133]CFBNCR En este punto la principal observación consiste en destacar que la resiliencia operativa digital de una organización no consiste solamente en la disponibilidad de activos tecnológicos o personal técnico, sino que considera elementos más integrales relacionados con el talento humano, los procesos y la orientación al servicio por parte de toda la organización; de manera que las organizaciones supervisadas deben fortalecer sus	**[133] No procede** En el artículo 1 de la propuesta de modificación reglamentaria se indica que esta se tendrá como plenamente integrada y complementaria al marco de regulación vigente sobre gestión de riesgos de cada Superintendencia, por lo que uno de los aspectos que se deben considerar como parte del Marco de Administración de Riesgos de las entidades es la continuidad del negocio.	

	procesos de continuidad del negocio, basados en normas internacionales como la ISO 22301 e ISO 27001.En este contexto, se sugiere revisar la conveniencia de incorporar estos aspectos dentro del acuerdo del Reglamento general de gobierno y gestión de la tecnología de información; o por el contrario, valorar si sería mejor fortalecer estos aspectos en los acuerdos que regulan el Gobierno Corporativo de las organizaciones supervisadas, de manera que se logre un alcance más integral a nivel estratégico y transversal en las organizaciones.		
	[134]CB Se solicita una revisión de los alcances consignados en estas secciones II, III y IV para claridad de todas las partes. Por ejemplo, no es competencia del Órgano de Dirección aplicar una evaluación, pero sí debe velar, supervisar y conocer los resultados de la evaluación y dimensionar los alcances. //////////////////////////Comentarios: Estas responsabilidades son propias del Comité de Tecnología de Información. Comentarios a los incisos d), e) y f): Las responsabilidades establecidas en los incisos d), e) y f) se consideran funciones muy técnicas y operativas que son vistas en el Comité (Comité de Tecnología o Comité de Seguridad de	**[134]Procede** Se atiende como parte de la observación [131 -a] y [131 –"d" y "f"]	

	Información), pero no son para el Órgano de Dirección.		
	[135]CCPA En los mismos términos del comentario anterior se puede sustituir la palabra asegurar, en congruencia con las buenas prácticas de Gobierno Corporativo.	**[135] No procede** Tanto en el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, como en la documentación emitida por el Comité de Supervisión Bancaria de Basilea, en relación con responsabilidades del Órgano de Dirección, así como en marcos de referencia internacionales como el caso de CobiT, utilizan el infinitivo "Asegurar" para denotar responsabilidades de gobierno.	
En relación con el gobierno de la seguridad de la información y de la seguridad cibernética, el Órgano de Dirección, al menos, debe:			En relación con el gobierno de la seguridad de la información y de la seguridad cibernética, el Órgano de Dirección, al menos, debe:
a) Asegurar que la gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética estén integrados dentro de la gestión de riesgos de la entidad o empresa supervisada.	**[136]FEDEAC** b) ¿Se ajustan las funciones del Comité de riesgos en el acuerdo 2-10? c) Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles. Incluir que el establecimiento y la definición del alcance de un sistema de gestión de seguridad de la información.	**[136] No procede** En el Acuerdo SUGEF 2-10, no se están realizando ajustes.	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) Asignar tiempo a las discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética en las reuniones del Órgano de Dirección.		Se modifica la redacción para mejorar el entendimiento de la disposición.	b) ~~Asignar~~ Promover y motivar las~~ tiempo a las~~ discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética en las reuniones del Órgano de Dirección.
c)Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles.	**[137]COOPEANDE** c) Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles. Incluir que el establecimiento y la definición del alcance de un sistema de gestión de seguridad de la información	**[137] No procede** La definición del alcance es parte de las tareas y actividades propias de las prácticas de CobiT 2019, así como en las declaraciones de la Norma ISO 27001. El artículo 31 "Sistema de gestión de seguridad de la información", entre otras disposiciones indica que:	c)Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles.

		Las entidades y empresas supervisadas deben diseñar, implementar, mantener y monitorear un sistema de gestión de la seguridad de la información que incluya las disposiciones de seguridad cibernética del presente reglamento.	
d) Asegurar que se apliquen medidas para la atención de los incidentes de seguridad de la información y de seguridad cibernética.	**[138]CATHAY** "Asegurar que se apliquen medidas para la atención de los incidentes de seguridad de la información y de seguridad cibernética." Una función de gestión de muy bajo nivel para ser asignada a un órgano de gobernanza. Debe asegurarse que se han atendido los incidentes de seguridad. "Asegurar que los requerimientos de seguridad de la información y de seguridad cibernética de la entidad o empresa supervisada sean de cumplimiento por parte de los proveedores de bienes y servicios de TI." Igual que el comentario anterior, es una tarea de gestión técnica no propia de un órgano director. Al cuerpo de gobierno le corresponde asegurarse que existan el SGSI que establece los controles a ser implementados (interno o externamente).	**[138] Procede** Se atiende como parte de la consulta [131 -a] y [131 –"d" y "f"]	~~d) Asegurar que se apliquen medidas para la atención de los incidentes de seguridad de la información y de seguridad cibernética.~~
e) Aprobar los planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética.	**[139]BCR** • Inciso e). Aclarar si los planes de cultura se deberán llevar a los distintos órganos de dirección considerando la figura corporativa.	**[139] No procede** Los mecanismos de aprobación se deben adaptar al tamaño, complejidad y modelo de negocio de la entidad o empresa supervisada. El Acuerdo CONASSIF 4-16, "Reglamento de Gobierno Corporativo", indica entre otros aspectos que el Órgano de Dirección debe establecer comités técnicos.	d~~e)~~ Aprobar los planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética.

		Asimismo, que dichos comités deben contar con una normativa, que regule su funcionamiento, integración, el alcance de sus funciones, y los procedimientos de trabajo, esto incluye la forma en que informará al Órgano de Dirección.	
f) Asegurar que los requerimientos de seguridad de la información y de seguridad cibernética de la entidad o empresa supervisada sean de cumplimiento por parte de los proveedores de bienes y servicios de TI.	**[140]ISTMO** Inciso f) Esta función no debería de ser del órgano de dirección, debe recaer en un órgano de menor nivel, como un comité de TI o comité de seguridad.	**[140] Procede** Se atiende como parte de la consulta [131 -a] y [131 –"d" y "f" **]**	~~f) Asegurar que los requerimientos de seguridad de la información y de seguridad cibernética de la entidad o empresa supervisada sean de cumplimiento por parte de los proveedores de bienes y servicios de TI.~~
Artículo 10. Responsabilidades sobre la resiliencia operativa digital	**[141]Luis Diego León Barquero** De acuerdo con las buenas prácticas de Gobierno Corporativo, sobre las responsabilidades principales de la Junta Directiva (estrategia, riesgos y cumplimiento), yo lo redactaría de la siguiente manera: En relación con el gobierno de la resiliencia operativa digital, el Órgano de Dirección, al menos, debe: a) Supervisar la resiliencia operativa digital para la continuidad de las operaciones de la entidad o empresa supervisada. b) Aprobar la estrategia de la resiliencia operativa digital. c) Aprobar los presupuestos y recursos necesarios para la implementación de la estrategia de resiliencia operativa digital. d) Supervisar que se implementen planes de respuesta, recuperación y atención de crisis para gestionar los incidentes de seguridad cibernética que podrían interrumpir la ejecución de los	**[141] No procede** Tanto en el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, como en los marcos de referencia internacionales, por ejemplo, CobiT, utilizan el infinitivo "Asegurar" para denotar responsabilidades de gobierno.	**Artículo 10. Responsabilidades sobre la resiliencia operativa digital**

	procesos críticos. e) Supervisar que los planes de respuesta de incidentes de seguridad cibernética sean acordes con el apetito de riesgo y la tolerancia establecida por la entidad o empresa supervisada. Es necesario separar las funciones y responsabilidades del órgano de Gobierno de las funciones y responsabilidades de la administración.		
	[142]MUCAP 1) El criterio es muy amplio, no inconcluso lo que puntualmente debe hacer el Órgano de Dirección al respecto. 2) Surge la duda si este criterio corresponde a lo que en la actualidad se define como estrategia de Continuidad del Negocio. No queda claro si lo que se está indicado sobre "resiliencia operativa digital", es lo que actualmente se trata como Continuidad de Tecnologías de Información. 3) Se deberá entender esta responsabilidad solo en función de los incidentes de seguridad cibernética, o para cualquier incidente, incluyendo los de ciberseguridad, esto debido a que no queda claro el alcance indicado en este inciso. 4) Se puede mencionar que se deja a interpretación que cuando se hace referencia a "Asegurar" por parte del Órgano de Dirección, es en el cumplimiento de aprobar la	**[142]Procede** 1- Se modifica la redacción para mejorar el entendimiento de la disposición considerando parte de las observaciones. 2-Por otra parte, la resiliencia operativa es la capacidad de una organización para resistir una disrupción repentina y recuperarse. Antes, ese concepto era sinónimo de continuidad del negocio o recuperación de desastres. Pero gracias a la digitalización de los negocios, la resiliencia operativa se convirtió en algo más profundo: una mezcla de continuidad del negocio, gestión de riesgos de proveedores, ciberseguridad y más**.** 3-En relación con lo indicado en el punto 3, se ajustó la redacción para aclarar el asunto. 4- Tanto el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, y marcos de referencia internacionales como el caso de CobiT, utilizan el infinitivo "Asegurar" para denotar responsabilidades de gobierno	

	normativa que se sustente a ese alcance, ya que como se indicó no es un órgano operativo.		
	[143]BAC Pregunta ¿Es posible tener un detalle o definición del tipo de servicios sujetos a lo denominado como operativa digital? ¿A qué tipo de servicios se apunta?	**[143]No procede** Se atiende como consulta. Respuesta: a. El reglamento indica que un activo digital es cualquier tipo de dato o activo de información que se presente en formato digital, que sea propiedad de una entidad o empresa supervisada o de sus partes interesadas y que permiten a estas mantener sus operaciones digitales y tecnológicas. b. Adicionalmente, indica que resiliencia operativa digital es la 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. c.En virtud de lo anterior, las entidades o empresas supervisadas deben definir cuales bienes y servicios relacionados a los activos digitales pueden ser considerados para mantener una resiliencia digital operativa en función del tamaño, complejidad y modelo de negocio.	
	[144]VIDAPLENA A lo largo de diferentes puntos del Reglamento general de gobierno y gestión de la tecnología de la información, acuerdo CONASSIF 5-24 se hace mención o solo	**[144] Procede** Se ajusta la redacción.	

	utilizan el apetito y tolerancia, pero no consideran o hacen mención sobre el nivel de capacidad en el momento de establecer los niveles de riesgo.		
	145]CFBNCR En este punto la principal observación consiste en destacar que la resiliencia operativa digital de una organización no consiste solamente en la disponibilidad de activos tecnológicos o personal técnico, sino que considera elementos más integrales relacionados con el talento humano, los procesos y la orientación al servicio por parte de toda la organización; de manera que las organizaciones supervisadas deben fortalecer sus procesos de continuidad del negocio, basados en normas internacionales como la ISO 22301 e ISO 27001.En este contexto, se sugiere revisar la conveniencia de incorporar estos aspectos dentro del acuerdo del Reglamento general de gobierno y gestión de la tecnología de información; o por el contrario, valorar si sería mejor fortalecer estos aspectos en los acuerdos que regulan el Gobierno Corporativo de las organizaciones supervisadas, de manera que se logre un alcance más integral a nivel estratégico y transversal en las organizaciones.	**[145]No procede** La resiliencia operativa es la capacidad de una organización para resistir una disrupción repentina y recuperarse. Antes, ese concepto era sinónimo de continuidad del negocio o recuperación de desastres. Pero gracias a la digitalización de los negocios, la resiliencia operativa se convirtió en algo más profundo: una mezcla de continuidad del negocio, gestión de riesgos de proveedores, ciberseguridad y más. Adicionalmente se aclara el término de activo digital.	
	[146]ABC No se observa en los lineamientos generales normas sobre el	**[146]No procede** Se elimina las referencias a la estrategia operativa digital, en relación con las	

	contenido general que se espera en la Estrategia de Resiliencia Operativa Digital. Si bien es recomendable mantener un amplio margen de flexibilidad para que las entidades adopten esta Estrategia de forma discrecional, según sus características organizacionales y apetito de riesgo, es importante comprender qué tipo de temas considera el Regulador que pueden formar parte de esta Estrategia, que no estén ya contemplados en otras de las Políticas, marcos y procedimientos que exige este Reglamento. Tampoco se incluye un detalle o definición del tipo de servicios sujetos al concepto de "operativa digital".	operaciones digitales y los servicios se incluyen los comentarios como parte de la respuesta de la observación [143].	
	[147]CB Inciso a): Comentarios: Esta tarea tampoco corresponde al Órgano de Dirección. Inciso b): Comentarios: Esta función no corresponde al Órgano de Dirección, pues eso es más operativo. Lo que sí puede hacer la Junta es aprobar lo que presente la Administración.	**[147] Procede** Se modifica de forma integral las responsabilidades y se alinean al Reglamento de Gobierno Corporativo, la continuidad del negocio, y la resiliencia operativa digital. Adicionalmente, se agrega la definición de activo digital para aclarar el entendimiento de la disposición.	
	[148]BCR Artículo 10. ¿Cuál es el contenido mínimo de la estrategia de resiliencia operativa digital? ¿Cuál es el marco de referencia donde se pueden encontrar las mejores prácticas para la definición de la estrategia de resiliencia operativa digital?	**[148] No procede** Lo dispuesto en relación con la estrategia de resiliencia operativa se excluyó y se modificaron las responsabilidades como parte de la respuesta de la observación [143].	
	[149]CCPA En los mismos términos del comentario anterior se puede	**[149] No procede** Tanto el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16,	

	sustituir la palabra asegurar, en congruencia con las buenas prácticas de Gobierno Corporativo.	y los marcos de referencia internacionales como el caso de CobiT, utilizan el infinitivo "Asegurar" para denotar responsabilidades de gobierno	
En relación con el gobierno de la resiliencia operativa digital, el Órgano de Dirección, al menos, debe:			En relación con el gobierno de la resiliencia operativa digital, el Órgano de Dirección, al menos, debe:
a) Asegurar la resiliencia operativa digital para la continuidad de las operaciones de la entidad o empresa supervisada.		Se modifica la redacción para mejorar el entendimiento de la disposición considerando parte de las observaciones.	a)~~Asegurar~~ Aprobar las políticas de resiliencia operativa digital~~—para la continuidad de las operaciones~~ de la entidad o empresa supervisada~~.~~
b) Establecer y aprobar la estrategia de la resiliencia operativa digital.	**[150]CATHAY Pregunta** "Establecer y aprobar la estrategia de la resiliencia operativa digital." ¿Cuáles son las directrices para establecer la estrategia de resiliencia operativa digital?	**[150] No procede** Lo dispuesto en relación con la estrategia de resiliencia operativa se excluyó y se modificaron las responsabilidades como parte de la respuesta de la observación [143]	b~~) Establecer y aprobar la estrategia de~~ 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 la implementación de la estrategia de resiliencia operativa digital.			c)Aprobar los presupuestos y recursos necesarios para asegurar la ~~implementación de la estrategia de~~ resiliencia operativa digital.
d)Asegurar que se implementen planes de respuesta, recuperación y atención de crisis para gestionar los incidentes de seguridad cibernética que podrían interrumpir la ejecución de los procesos críticos.	**[151]BPDC** Para los puntos d y e, se considera que el alcance no debería estar restringido únicamente a incidentes de seguridad, sino a cualquier incidente que interrumpa la ejecución de los procesos críticos	**[151] Procede** **S**e modificaron conforme a la observación [143], adicionalmente se incorpora el concepto de activo digital.	d)Asegurar que se implementen planes de respuesta, recuperación y atención de crisis para gestionar los incidentes relacionados con los activos digitales ~~de seguridad cibernética~~ que podrían interrumpir la ejecución de los procesos críticos.
e) Asegurar que los planes de respuesta de incidentes de seguridad cibernética sean acordes con el apetito de riesgo y la tolerancia establecida por la entidad o empresa supervisada.		Se modifica la redacción para mejorar el entendimiento de la disposición considerando parte de las observaciones.	e) Asegurar que los planes de respuesta de incidentes relacionados con los activos digitales ~~de incidentes de seguridad cibernética~~ sean acordes con el apetito, ~~de riesgo y~~ ~~la~~ tolerancia y capacidad de riesgo establecid~~a~~os 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:	**[152]CFBNCR** Para los artículos 8,9,10,11,13,14 y 15 Se sugiere revisar la pertinencia de algunas	**[152] Procede** Se aclara que las responsabilidades establecidas en la presente propuesta reglamentaria complementan y	En relación con el gobierno y la gestión de TI, la Alta Gerencia, al menos, debe:

	responsabilidades establecidas en las secciones II, III y IV, dada la existencia del principio de proporcionalidad. Enel entendido que, en apego a las facultades definidas por ley, el órgano de dirección tiene funciones asociadas principalmente a la aprobación de políticas, el apetito de riesgo, reglamentos, la estrategia de la entidad, asignar responsabilidades y recursos, entre otros y es responsabilidad de la administración activa su ejecución, además de alinear los procesos, procedimientos, registros a los criterios aprobados por el órgano. Dicho lo anterior, se considera que algunas funciones están utilizando verbos descritos en términos de funciones administrativas y operativas que son más bien responsabilidad del Administración, y no del órgano de dirección ni de los comités de apoyo. Por ejemplo, no es competencia del órgano de dirección el aplicar una evaluación, pero sí debe velar porque se establezca, supervisar y conocer los resultados de la evaluación y dimensionar los alcances. En ese sentido, se sugiere una revisión integral de los alcances consignados en esas secciones, para una adecuada asignación de responsabilidades, conforme al rol de cada una de las partes y las mejores prácticas. Para efectos de facilitar la aplicación del acuerdo en cuestión, se	refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta. Se ajustan algunas de las responsabilidades con los infinitivos correspondientes al órgano de dirección, además, se aclara que tanto el Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, y los marcos de referencia internacionales como el caso de CobiT, utilizan el infinitivo "Asegurar" para denotar responsabilidades de gobierno.	

	recomienda que los lineamientos de la gestión de los procesos sobre la seguridad de la información y la seguridad cibernética, evaluación de las necesidades de las partes interesadas y la estrategia para la resiliencia operativa digital estén contenidas en el marco de gobierno y gestión de TI, donde se delimiten las responsabilidades de las partes involucradas en su ejecución. Aplicando esta recomendación, podría generarse un único artículo de responsabilidades que se homologuen o alineen en estructura y alcance a otros reglamentos vigentes como: CONASSIF 4-16, CONASSIF 12-21 y SUGEF 2-10.Respecto a la gestión del comité de TI, también le aplica el principio de proporcionalidad por lo que se sugiere alinear su gestión al artículo 24 del acuerdo CONASSIF 4-16 Reglamento de Gobierno Corporativo y no concentrar sus funciones en aspectos administrativos que son responsabilidad de la Administración, pero sí es responsabilidad de la Administración el rendir cuentas de la gestión de aplicación del marco de gobierno y gestión de TI que incluyan aspectos como resultados de evaluaciones al proceso, ya sean internas o externas, implementación de la estrategia, indicadores de desempeño, entre otros.		

	[153]CB La formulación y aprobación de estrategias de TI y la asignación de recursos que debe proponer la Alta Gerencia, pueden resultar en una carga administrativa considerable, especialmente si las estrategias deben revisarse y aprobarse con frecuencia por el Órgano de Dirección. Se sugiere al Regulador un marco que permita flexibilidad operativa en la gestión de TI, sin necesidad de aprobaciones constantes por parte del Órgano de Dirección.	**[153]No Procede** La propuesta de modificación 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, así mismo, esta disposición forma parte del actual reglamento de TI CONASSIF 5-17. Por otra parte, las disposiciones se alinean con los aspectos normados en el Acuerdo CONASSIF 4-16.	
a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección.	**[154]COOPEANDE** a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección, con base en el alcance aprobado por el Órgano de Dirección.	**[154]No procede** La redacción indica que se trata del marco de gobierno y gestión de TI aprobado por el Órgano de Dirección, por lo que el alcance que dicho marco contiene deberá ser conocido previamente por el Órgano de Dirección.	a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección.
	[155]FEDEAC a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección, con base en el alcance aprobado por este Órgano. e) Se sugiere incorporar que la Alta Gerencia es la responsable de diseñar e implementar los planes de acción que se originen por incidentes de Seguridad de la Información, Seguridad Cibernética, resiliencia operativa digital y continuidad de negocio.	**[155] No procede** a-La redacción indica que se trata del marco de gobierno y gestión de TI aprobado por el Órgano de Dirección, por lo que el alcance que dicho marco contiene deberá ser conocido previamente por el Órgano de Dirección. e-Las entidades y empresas supervisada para la atención de los incidentes deben seguir las disposiciones establecidas en la Sección II. Incidentes de seguridad cibernética. Adicionalmente es responsabilidad de las entidades y empresas supervisadas establecer las estructuras que diseñen e implemente los temas relacionados con la seguridad de la información y la seguridad cibernética de conformidad con lo dispuesto en el artículo 34.	

		Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de seguridad cibernética.	
b) Proponer al Órgano de Dirección las estrategias y los recursos requeridos para la implementación del marco de gobierno y gestión de TI.	**[156]ABC** La formulación y aprobación de estrategias de TI, así como la asignación de recursos que debe proponer la Alta Gerencia, pueden resultar en una carga administrativa considerable, especialmente si las estrategias deben revisarse y aprobarse con frecuencia por el Órgano de Dirección. Por ello, se considera que se debe establecer un marco que permita cierta flexibilidad operativa en la gestión de TI, sin necesidad de aprobaciones constantes por parte del Órgano de Dirección.	**[156]No procede** Las disposiciones se alinean con los aspectos normados en el Acuerdo CONASSIF 4-16. 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, así mismo, esta disposición forma parte del actual reglamento de TI CONASSIF 5-17.	b) Proponer al Órgano de Dirección las estrategias y los recursos requeridos para la implementación del marco de gobierno y gestión de TI.
c)Implementar las políticas relacionadas con TI aprobadas por el Órgano de Dirección.			c)Implementar las políticas relacionadas con TI aprobadas por el Órgano de Dirección.
d)Designar las áreas de negocio y de TI responsables de implementar el marco de gobierno y de gestión TI.	**[157]Luis Diego León Barquero** Yo cambiaría el inciso d del artículo 11: b) Designar las áreas de negocio y de TI responsables de implementar el marco de gestión de TI. Se eliminó que la alta administración designe los responsables de implementar el marco de Gobierno de TI, pues esta es una responsabilidad del órgano de gobierno. Es necesario separar las funciones y responsabilidades del órgano de Gobierno de las funciones y responsabilidades de la administración.	**[157]Procede** Para ser consistentes con las disposiciones del Acuerdo CONASSIF 4-16, se traslada y modifica esta disposición a las responsabilidades generales del gobierno de TI Articulo 8.	~~d)Designar las áreas de negocio y de TI responsables de implementar el marco de gobierno y de gestión TI~~.
	[158]COOPEALIANZA	**[158]No Procede**	

	Nótese que el punto d) indica que la Alta Gerencia, designa las áreas de negocio y de TI responsables de implementar el marco de gobierno y de gestión TI, lo anterior refuerza, el aspecto de que este es un marco de gobierno y gestión empresarial y no sólo de TI.	Las disposiciones establecidas en la propuesta buscan reforzar un involucramiento de los Órganos de Dirección en temas de tecnologías de información, seguridad de la información, seguridad cibernética, gestión de riesgos de la cadena de proveedores, así como gestión de riesgos de nuevas tecnologías y computación en la nube.	
e) Implementar los planes de acción para la atención de los hallazgos de la auditoría externa de TI.			de) Implementar los planes de acción para la atención de los hallazgos de la auditoría externa de TI.
		Se incluye considerando parte de las observaciones para trasladar responsabilidades que estaban asignadas al Órgano de Dirección y que lo correcto es que sean responsabilidades de la Alta Gerencia.	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.
		Se incluye considerando parte de las observaciones para trasladar responsabilidades que estaban asignadas al Órgano de Dirección y que lo correcto es que sean responsabilidades de la Alta Gerencia.	f) Establecer las medidas para la gestión de los incidentes de seguridad de la información y de seguridad cibernética.
		Se incluye considerando parte de las observaciones para trasladar responsabilidades que estaban asignadas al Órgano de Dirección y que lo correcto es que sean responsabilidades de la Alta Gerencia.	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.
		Se incluye considerando parte de las observaciones para trasladar responsabilidades que estaban asignadas al Órgano de Dirección y que lo correcto es que sean responsabilidades de la Alta Gerencia.	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.	**[159]JUPEMA** ¿Se incluirá en el acuerdo Conassif 4-16 como uno de los comités técnicos?	**[159]No procede** Se atiende como consulta. El artículo 6 del Reglamento de Gobierno Corporativo, Acuerdo	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.

	¿Cómo debe estar conformado el Comité de TI? ¿En el Comité de TI quién con voto?	CONASSIF 4-16, indica que el Órgano de Dirección es el responsable de aprobar la estructura organizacional y funcional de la entidad y proporcionar los recursos necesarios para el cumplimiento de sus responsabilidades. Esto implica, entre otros aspectos, que: Constituye y establece 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. Con base en lo anterior, se considera que no es necesario incluir el Comité de TI o función equivalente dentro del Acuerdo CONASSIF 4-16, que el citado artículo faculta al Órgano de Dirección para que pueda constituir comités técnicos.	
	[160]FEDEAC Pregunta ¿El Comité de TI se incluirá en el acuerdo Conassif 4-16 como uno de los comités técnicos de apoyo al Órgano de Dirección? ¿Cómo debe estar conformado el Comité de TI, quiénes con voto, de tal manera que no quede a interpretación de los supervisados y no surjan hallazgos por diferencias entre la expectativa del supervisor y del supervisado por la conformación de este comité? Se entiende entidades con subsidiarias pueden contar con un único marco de gobierno y gestión de TI, pero en el caso que a una subsidiaria no le apliquen la	**[160]No procede** Se atiende como consulta. El artículo 6 del Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, indica que el Órgano de Dirección es el responsable de aprobar la estructura organizacional y funcional de la entidad y proporcionar los recursos necesarios para el cumplimiento de sus responsabilidades. Esto implica, entre otros aspectos, que: Constituye y establece 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	

	totalidad de procesos, ¿se puede limitar el alcance del marco de gobierno y gestión de TI para esa empresa en particular?	de los recursos, independencia, autoridad y jerarquía necesarios para su operación. Con base en lo anterior, se considera que no es necesario incluir el Comité de TI o función equivalente dentro del Acuerdo CONASSIF 4-16, que el citado artículo faculta al Órgano de Dirección para que pueda constituir comités técnicos.	
	[161]COOPEBANPO Este artículo impone la obligación de contar con un comité de TI, pero deja un poco escueta la definición de "función equivalente" creo que, para efectos normativos, la norma debería ser clara y concisa en lo que se quiere del supervisado. Así como queda, la interpreto como: no tengo un comité de ti, pero debo tener una función equivalente, o sea que tengo que crear una estructura interna conformada con criterios de la empresa, que a lo mejor no cumpla con lo que se desea por parte del supervisor. cuando se refieren a función equivalente, ¿en qué están pensando?	**[161]No procede** El término equivalente es ampliamente utilizado en el Reglamento de Gobierno Corporativo. Equivalente es un adjetivo que expresa algo que tiene igual valor, estimación, potencia o significado. Que supone o implica igualdad o paridad en eficacia, valor, estimación, atribución o categoría. || En cuestiones idiomáticas o de traducción, que significa lo mismo o que son muy parecidos en sus significados. En virtud de lo anterior, las entidades y empresas supervisadas en función del tamaño, complejidad, modelo de negocio y sus riesgos, podrán valorar la asignación de las funciones del comité de TI en una función equivalente, la cual debe cumplir con las responsabilidades asignadas a dicho comité.	
	[162]CAJAANDE Pregunta Actualmente se cuenta con representación de Riesgos y de Auditoría de TI en el Comité de TI, dado regulaciones anteriores, al quedar a decisión del propio grupo o conglomerado financiero quién integra el comité, ¿ya no es necesario la participación de estos órganos de control tanto en un Comité de TI corporativo o el actual Comité de TI?	**[162]No procede** Se atiende como consulta. a. El artículo 6 del Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, indica que el Órgano de Dirección es el responsable de aprobar la estructura organizacional y funcional de la entidad y proporcionar los recursos necesarios para el cumplimiento de sus responsabilidades. b. Lo anterior implica, entre otros aspectos, que: Constituye y establece 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. c.Adicionalmente, el artículo 12 indica entre otras disposiciones 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.	
	[163]INS Se estima que se le están otorgando al Supervisor facultades que son propias de la administración de las entidades supervisadas, por cuanto en las tres normas, en ese respectivo orden, se faculta al supervisor para requerir: conformación de comité de TI individual, gestiones de TI individuales, así como infraestructuras de almacenamiento diferentes a las adoptadas por las supervisadas.	**[163] No procede** El supervisor tiene la facultad de solicitar cambios si observa una gestión inadecuada dentro de la organización. Los supervisores cumplen un rol de verificar que las operaciones se realicen de manera eficiente y conforme a los estándares establecidos. Cuando identifican problemas o áreas que necesitan mejoras, tienen la responsabilidad de informar y recomendar ajustes o cambios para optimizar el desempeño. En virtud de lo anterior se incluyen en la propuesta disposiciones para la superintendencia y para las entidades, las cuales están en función de sus riesgos, tamaño, complejidad y modelo de negocio.	
	[164]CFBNCR Para los artículos 8,9,10,11,13,14 y 15 Se sugiere revisar la pertinencia de algunas	**[164]No procede** Las responsabilidades establecidas en la presente propuesta reglamentaria complementan y refuerzan los	

	responsabilidades establecidas en las secciones II, III y IV, dada la existencia del principio de proporcionalidad. Enel entendido que, en apego a las facultades definidas por ley, el órgano de dirección tiene funciones asociadas principalmente a la aprobación de políticas, el apetito de riesgo, reglamentos, la estrategia de la entidad, asignar responsabilidades y recursos, entre otros y es responsabilidad de la administración activa su ejecución, además de alinear los procesos, procedimientos, registros a los criterios aprobados por el órgano. Dicho lo anterior, se considera que algunas funciones están utilizando verbos descritos en términos de funciones administrativas y operativas que son más bien responsabilidad del Administración, y no del órgano de dirección ni de los comités de apoyo. Por ejemplo, no es competencia del órgano de dirección el aplicar una evaluación, pero sí debe velar porque se establezca, supervisar y conocer los resultados de la evaluación y dimensionar los alcances. En ese sentido, se sugiere una revisión integral de los alcances consignados en esas secciones, para una adecuada asignación de responsabilidades, conforme al rol de cada una de las partes y las mejores prácticas.	mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta. Se ajustan algunas de las responsabilidades con los infinitivos correspondientes al Órgano de Dirección, adicionalmente, se aclara que el término asegurar se utiliza según las prácticas de CobiT, para los procesos de Gobierno, adicionalmente, se hace referencia en el reglamento de Gobierno Corporativo y en la documentación emitida por el Comité de Supervisión Bancaria de Basilea, en relación con responsabilidades del Órgano de Dirección.	

	Para efectos de facilitar la aplicación del acuerdo en cuestión, se recomienda que los lineamientos de la gestión de los procesos sobre la seguridad de la información y la seguridad cibernética, evaluación de las necesidades de las partes interesadas y la estrategia para la resiliencia operativa digital estén contenidas en el marco de gobierno y gestión de TI, donde se delimiten las responsabilidades de las partes involucradas en su ejecución. Aplicando esta recomendación, podría generarse un único artículo de responsabilidades que se homologuen o alineen en estructura y alcance a otros reglamentos vigentes como: CONASSIF 4-16, CONASSIF 12-21 y SUGEF 2-10.Respecto a la gestión del comité de TI, también le aplica el principio de proporcionalidad por lo que se sugiere alinear su gestión al artículo 24 del acuerdo CONASSIF 4-16 Reglamento de Gobierno Corporativo y no concentrar sus funciones en aspectos administrativos que son responsabilidad de la Administración, pero sí es responsabilidad de la Administración el rendir cuentas de la gestión de aplicación del marco de gobierno y gestión de TI que incluyan aspectos como resultados de evaluaciones al proceso, ya sean internas o		

	externas, implementación de la estrategia, indicadores de desempeño, entre otros.		
	[165]BCR Pregunta • ¿Deberá participar personas de negocio de las subsidiarias en el Comité de TI? • ¿podría el gerente general de cada sociedad definir un representante de negocio? • Se solicita ampliar la conformación del comité de TI y presidencia del Comité.	**[165]No procede** Se atiende como consulta. a. El artículo 6 del Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, indica que el Órgano de Dirección es el responsable de aprobar la estructura organizacional y funcional de la entidad y proporcionar los recursos necesarios para el cumplimiento de sus responsabilidades. b. Lo anterior implica, entre otros aspectos, que: Constituye y establece 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. c. Adicionalmente, el artículo 12 de esta propuesta indica entre otras disposiciones 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.	
	[166]ISACA ¿Por qué trasladar la responsabilidad a la entidad o empresa supervisada de conformar un Comité de TI?, este es una agrupación que se exige hace décadas, ya es conocida su	**[166] No Procede** Las disposiciones se alinean con los aspectos normados en el Acuerdo CONASSIF 4-16. La propuesta reglamentaria contiene las expectativas de alto nivel que las superintendencias esperan que las	

	conformación, una normativa debe evitar ser una metodología, es decir que en la normativa debería indicarse como se conforma el Comité, cuáles son los puestos básicos, cuáles posibles puestos dependiendo del tipo de entidad y una serie de homologaciones. Precisamente, este tipo de normativas dejan varios controles vitales a discreción, y es el momento de dictar lineamientos estandarizados para que, en este caso, un Comité de TI esté conformado exactamente de la misma forma y alcance en todas las empresas que son de la misma naturaleza, como los bancos o como las cooperativas.	entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. Además, se aclara que, las entidades y empresas supervisadas varían en naturaleza jurídica, tamaño, perfil de riesgo, enfoque de negocio, volumen y complejidad de sus operaciones. En este sentido, esta propuesta normativa busca dejar de lado el modelo de cumplimiento tradicional basado en reglas y migrar a un modelo basado en riesgos, donde los controles se diseñen e implementen de conformidad con las particularidades de cada organización.	
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.	**[167]COOPEMEP** Se solicita eliminar la tipificación del Comité de TI corporativo y dejar solo la tipificación de la gestión de TI pues queda supeditado a tener un comité de TI corporativo solo si se tiene una gestión de TI corporativa que cumple los requisitos (esto puede entorpecer las articulaciones de los conglomerados que no son corporativos pero que necesitan un Comité que articule)	**[167] No procede** La unidad de TI puede determinar si realiza gestión de TI corporativa, ya que de forma predetermina la gestión es tipificada como individual. Para tipificar la gestión corporativa se debe cumplir con los requisitos establecidos en los lineamientos. Por otra parte, se puede establecer un comité de TI corporativo si se cumple con los requisitos y si la gobernanza lo requiere se podrán establecer otros comités para labores de coordinación tal como lo indica el reglamento de gobierno corporativo.	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.
	[168]CIS Solicitar eliminar la tipificación del comité de TI corporativo y dejar solo la tipificación de la gestión de TI pues queda supeditado a tener un comité de TI corporativo solo si se tiene una	**[168] No procede** La unidad de TI puede determinar si realiza gestión de TI corporativa, ya que de forma predetermina la gestión es tipificada como individual.	

	gestión de TI corporativa que cumple los requisitos (esto puede entorpecer las articulaciones de los conglomerados que no son corporativos pero que necesitan un Comité que articule)Ver en el reglamento "Las condiciones para tipificar un Comité de TI como corporativo están establecidas en los lineamientos generales del presente reglamento. "Ver en los lineamientos: "Objetivo: Establecer las condiciones para tipificar la gestión de TI, el Comité de TI o sus funciones equivalentes como corporativos. Las condiciones que las entidades y empresas supervisadas considerarán para tipificar su gestión de TI, Comité de TI o funciones equivalentes como corporativos son las siguientes..."	Para tipificar la gestión corporativa se debe cumplir con los requisitos establecidos en los lineamientos. Por otra parte, se puede establecer un comité de TI corporativo si se cumple con los requisitos y si la gobernanza lo requiere se podrán establecer otros comités para labores de coordinación tal como lo indica el reglamento de gobierno corporativo.	
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 un Comité individual de TI para la respectiva entidad o empresa.			En el caso de que se determine que el Comité de TI corporativo no atiende en forma adecuada y oportuna las funciones y obligaciones indicadas en este reglamento, para alguna de las entidades o empresas que constituyen el grupo o conglomerado, la Superintendencia responsable de la supervisión de dicha entidad o empresa puede requerir que se proceda con la conformación de un Comité individual de TI para la respectiva entidad o empresa.
Artículo 13. Responsabilidades del Comité de TI o de la función equivalente			**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:	**[169]MUCAP**	**[169] Procede** Se ajusta la redacción del inciso e.	Corresponden al Comité de TI o a la función equivalente, al menos, las siguientes responsabilidades:

	Se destaca que el Comité de TI es un órgano de control del Órgano de Dirección, al ser este tipo de documentación, de carácter operativo, la aprobación es realizada por de Jefaturas, directores o Alta Gerencia.		
	[170]FEDEAC a) Supervisar la implementación del marco de gobierno y gestión de TI, con base en el alcance aprobado por el Órgano de Dirección. e) Aprobar los procedimientos, los instructivos y la documentación operativa de TI. Incluir esta responsabilidad en el Comité de TI es de poco valor agregado y genera atrasos en el proceso, es importante que el Comité de TI recomiende al Órgano de Dirección la aprobación de documentos más estratégicos como reglamentos y políticas, y no incluir documentos operativos. g) Definir el término de tecnologías emergentes en el artículo de definiciones. h) ¿Cuál es el alcance de este estudio técnico? ¿Quién lo ejecuta?, ¿qué pasa con las subsidiarias, son estudios diferentes?	**[170] No procede** a-La redacción indica que se trata del marco de gobierno y gestión de TI aprobado por el Órgano de Dirección, por lo que el alcance que dicho marco contiene fue conocido previamente por el Órgano de Dirección. e-Se ajustó la redacción del inciso e. g-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. h-Se ajustó la redacción del lineamiento para aclarar el tema de las subsidiarias.	
	[171]CFBNCR Para los artículos 8,9,10,11,13,14 y 15Se sugiere revisar la pertinencia de algunas responsabilidades establecidas en las secciones II, III y IV, dada la existencia del principio de proporcionalidad. Enel entendido	**[171] Procede** Se ajustan algunas de las responsabilidades con los infinitivos correspondientes al Órgano de Dirección. Las responsabilidades establecidas en la presente propuesta reglamentaria complementan y refuerzan los	

	que, en apego a las facultades definidas por ley, el órgano de dirección tiene funciones asociadas principalmente a la aprobación de políticas, el apetito de riesgo, reglamentos, la estrategia de la entidad, asignar responsabilidades y recursos, entre otros y es responsabilidad de la administración activa su ejecución, además de alinear los procesos, procedimientos, registros a los criterios aprobados por el órgano. Dicho lo anterior, se considera que algunas funciones están utilizando verbos descritos en términos de funciones administrativas y operativas que son más bien responsabilidad del Administración, y no del órgano de dirección ni de los comités de apoyo. Por ejemplo, no es competencia del órgano de dirección el aplicar una evaluación, pero sí debe velar porque se establezca, supervisar y conocer los resultados de la evaluación y dimensionar los alcances. En ese sentido, se sugiere una revisión integral de los alcances consignados en esas secciones, para una adecuada asignación de responsabilidades, conforme al rol de cada una de las partes y las mejores prácticas. Para efectos de facilitar la aplicación del acuerdo en cuestión, se recomienda que los lineamientos de la gestión de los procesos sobre la seguridad de la información y la seguridad cibernética, evaluación	mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta. Se ajustan algunas de las responsabilidades con los infinitivos correspondientes al órgano de dirección.	

	de las necesidades de las partes interesadas y la estrategia para la resiliencia operativa digital estén contenidas en el marco de gobierno y gestión de TI, donde se delimiten las responsabilidades de las partes involucradas en su ejecución. Aplicando esta recomendación, podría generarse un único artículo de responsabilidades que se homologuen o alineen en estructura y alcance a otros reglamentos vigentes como: CONASSIF 4-16, CONASSIF 12-21 y SUGEF 2-10.Respecto a la gestión del comité de TI, también le aplica el principio de proporcionalidad por lo que se sugiere alinear su gestión al artículo 24 del acuerdo CONASSIF 4-16 Reglamento de Gobierno Corporativo y no concentrar sus funciones en aspectos administrativos que son responsabilidad de la Administración, pero sí es responsabilidad de la Administración el rendir cuentas de la gestión de aplicación del marco de gobierno y gestión de TI que incluyan aspectos como resultados de evaluaciones al proceso, ya sean internas o externas, implementación de la estrategia, indicadores de desempeño, entre otros.		
	[172]COOPENAE Impacto Bajo, Esfuerzo Bajo) Define las funciones que debe llevar el Comité de TI como	**[172] No procede** Lo indicado en la observación es distinto a lo señalado en la propuesta de artículo.	

	componente de gobierno. No genera impacto o cambio significativo.		
	[173]CIS Se sugiere la exclusión de la función de "e) Aprobar los procedimientos, los instructivos y la documentación operativa de TI." pues es muy operativa y genera mucho volumen en los comités, es mejor asegurar la responsabilidad de cumplimiento con auditorías internas y autoevaluaciones.	**[173] Procede** Se ajusta la redacción del inciso e**.**	
a) Supervisar la implementación del marco de gobierno y gestión de TI.	**[174]COOPEANDE** a) Supervisar la implementación del marco de gobierno y gestión de TI, con base en el alcance aprobado por el Órgano de Dirección. e) Aprobar los procedimientos, los instructivos y la documentación operativa de TI. Incluir esta responsabilidad en el Comité de TI es de poco valor agregado y genera atrasos en el proceso, es importante que el Comité de TI recomiende al Órgano de Dirección la aprobación de documentos más estratégicos como reglamentos y políticas, y no incluir documentos operativos.	**[174]No procede** a-La redacción indica que se trata del marco de gobierno y gestión de TI aprobado por el Órgano de Dirección, por lo que el alcance que dicho marco contiene deberá set conocido previamente por el Órgano de Dirección. e-Se ajustó la redacción del inciso e.	a) Supervisar la implementación del marco de gobierno y gestión de TI.
	[175]CAJAANDE E. Se sugiere que la función se mantenga como la c) Proponer al órgano de Dirección las políticas relacionadas con TI o bien las del marco de gestión de TI. El aprobar documentación operativa puede generar una carga a un órgano que	**175] No procede** En la propuesta de modificación reglamentaria 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.	

	le competen funciones de más alto nivel. G. Favor ampliarnos sobre ¿Qué aspectos de las tecnologías emergentes se auditarían? Sobre este tema ¿Qué tipo de documentación se espera?	Por otra parte, se ajustó la redacción del inciso e. En relación con el aspecto G: Se espera que las entidades y empresas supervisadas diseñen y documenten las medidas de control (Administrativas y Técnicas), que permitan mitigar los riesgos asociadas a las tecnologías emergentes, dichas medidas estarán reveladas a través del perfil de TI y demás documentación dispuesta por la entidad, las cuales será validad por las AE de TI, de conformidad con el alcance comunicado por las Superintendencias. La documentación mínima esperada sobre tecnologías emergentes incluye al menos pero no limitado el diseño de políticas, procedimientos, instructivos, manuales, y formularios que permitan evidenciar los controles administrativos y técnicos relacionados a dichas tecnologías adoptadas por la organización dentro sus procesos de negocio para la entrega de bienes y servicios a sus partes interesadas.	
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.			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.	**[176]Luis Diego León Barquero** Puede existir una confusión con los incisos c y e sobre las responsabilidades del comité de TI: c) Proponer al Órgano de Dirección las políticas relacionadas con TI. e) Aprobar los procedimientos, los instructivos y la documentación operativa de TI. ¿Cuál es la diferencia entre las políticas relacionadas con TI y los procedimientos, los instructivos y	**[176] Procede** Se ajusta la redacción del inciso e.	c)Proponer al Órgano de Dirección las políticas relacionadas con TI.

	la documentación operativa de TI? ¿Por qué el Comité en algunos casos los aprueba procedimientos y en otros los propone políticas? No aparece en las definiciones la definición de políticas ni la definición de procedimientos, por lo que la redacción puede crear confusión.		
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.			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) Aprobar los procedimientos, los instructivos y la documentación operativa de TI.	**[177]BNCR** Respecto al punto "e" ¿es indispensable que el Comité de TI apruebe todos los documentos indicados en dicho punto, o se puede elevar el tema solamente como informativo (con un resumen de toda documentación que cambió) y que sean los directores de las áreas de Tecnología los que aprueben dicha documentación?	**[177] Procede** Se ajusta la redacción del inciso e.	e) ~~Aprobar~~ Validar que los procedimientos, los instructivos y la documentación ~~operativa~~ de TI sean implementados desde las unidades funcionales responsables de ejecutarlos.
	[178]BPDC Para el punto e se considera que esta es una tarea muy técnica de bajo nivel que le correspondería a cada dueño de proceso. Esta responsabilidad agrega burocracia adicional innecesaria porque el Comité NO es técnico.	**[178] Procede** Se ajusta la redacción del inciso e.	
	[179]COOPEMEP Se solicita la exclusión de la función de "e) Aprobar los procedimientos, los instructivos y la documentación operativa de TI." pues es muy operativa y genera mucho volumen en los comités, es mejor asegurar la	**[179] Procede** Se ajusta la redacción del inciso e.	

	responsabilidad de cumplimiento con auditorías internas y autoevaluaciones.		
	[180]CATHAY "La aprobación de procedimientos, instructivos y documentación operativa de TI" Debe estar asociado al responsable de la Unidad de TI, debido al alto componente técnico y con información sensible (IPs, configuración, versionado, etc) que es se expone en estos documentos. Bajo principios de "confianza cero" y "accesos con privilegio mínimo", la única información razonable que debe ser aprobada por un órgano de gobierno deben ser las políticas que conforman el marco de gestión de TI y que regularán las prácticas operativas de TI a cargo del responsable de la Unidad de TI. Se sugiere cambiar este lineamiento por Velar por el establecimiento y cumplimiento de procedimientos, instructivos y documentación operativa de TI alineados a los objetivos de gobierno y gestión".	**[180] Procede** Se ajusta la redacción del inciso e.	
	[181]COOPEBANPO Considerar la exclusión de la función de "e) Aprobar los procedimientos, los instructivos y la documentación operativa de TI." pues es muy operativa y genera mucho volumen en los comités, es mejor asegurar la responsabilidad de cumplimiento con auditorías internas y autoevaluaciones, que dicho sea	**[181] Procede** Se ajusta la redacción del inciso e.	

	de paso esa es su función, validar los controles y la oportunidad de los controles. Adicionalmente, elevar estos temas administrativos al Comité de TI podría suponer retrasos en la gestión administrativa dado que por lo general no sesión con regularidad. Debería ser potestades de la alta gerencia.		
	[182]COOPEALIANZA No estamos de acuerdo con el punto e), ya que, reduce la agilidad y eficiencia del negocio, al limitar la aprobación de la operativa que se encuentra en constante cambio y adaptación, un comité de TI o equivalente, lo que hace es orientar de manera estratégica a la gestión. Es importante que, como principio de gobierno, siempre exista una debida separación de las actividades para gobernar y de las actividades para gestionar.	**[182] Procede** Se ajusta la redacción del inciso e.	
	[183]VIDAPLENA Se solicita revisar o reconsiderar inciso e), dado que no le debería corresponder a un Comité de TI la aprobación de normativa técnica y relacionada con la operativa de las áreas de TI o del MGTI, lo anterior considerando que lo miembros del comité no necesariamente todos van a manejar información a un nivel técnico y operativo asociada al perfil. Además, deben tomar en cuenta que normalmente en las áreas de TI y del MGTI se generan una cantidad importante de documentos de tipo técnico(procedimientos,	**[183] Procede** Se ajusta la redacción del inciso e.	

	instructivos, registros, directrices, manuales, catálogos, lineamientos, entre otros) lo que implicaría asignar tiempo de un Comité en actividades que no necesariamente genera un valor agregado al trabajo que este órgano realiza, pero si puede afectar la revisión y análisis de temas, que si le conciernen a un órgano que funciona como apoyo a la Junta Directiva.		
	[184]POPULARPENSIONES Como parte de las funciones del Comité de TI en el inciso e) se asigna la aprobación de procedimientos, instructivos y demás documentación operativa. Esta documentación como se indica literalmente refiere a la operativa de TI, por lo cual es inconveniente que sea abarcado por un órgano de tan alto nivel como lo es un Comité de TI. Es importante anotar que la documentación que debería ser aprobada por este Comité debería ser lo referente a políticas y/o directrices.	**[184] Procede** Se ajusta la redacción del inciso e.	
	[185]OPC-CCSS Se menciona en el punto E) que el Comité de TI debe "aprobar los procedimientos, los instructivos y la documentación operativa de TI", se sugiere eliminar esta responsabilidad al ser un tema más de la administración y en lugar de eso, se podrían comunicar los cambios a este órgano, de ser necesario.	**[185] Procede** Se ajusta la redacción del inciso e.	
	[186]CB	**[186] Procede**	

	Sobre la responsabilidad que establece el inciso e), se considera que establece una tarea muy operativa y técnica que le correspondería a cada dueño de proceso, pero no al Comité de TI que es un órgano de control del Órgano de Dirección; de tal forma que, al ser este tipo de documentación de carácter operativo, la aprobación debe ser realizada por Jefaturas, Directores o Alta Gerencia, pero no por el Comité de TI.	Se ajusta la redacción del inciso e.	
	[187]BCR Inciso e. ¿Cuál es el nivel de detalle para la aprobación de procedimientos y documentos operativos? Eso puede generar una burocracia adicional que atrasa la emisión de documentos de trabajo. • Inciso e. ¿Es toda la normativa de TI?, ¿A qué se refiere con procedimientos, instructivos y documentación operativa? • 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.	**[187] Procede** Se ajusta la redacción del inciso e.	
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.			g) Validar que la firma de auditores externos o el profesional independiente de TI tengan los conocimientos y la experiencia para auditar aspectos de seguridad de la información, seguridad cibernética y tecnologías emergentes, de conformidad con el alcance solicitado.
h) Validar el estudio técnico en el que se fundamentan los procesos de evaluación del marco de gobierno y gestión de TI que no le aplican a la entidad o empresa supervisada.			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	**[188]Luis Diego León Barquero** Yo cambiaría el inciso a del artículo 14, pues habla de que la Auditoría Interna supervisa, cuando realmente ejecuta trabajos de revisión o aseguramiento. Cambiaría el inciso a del artículo 14 de la siguiente manera: a) Verificar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI. El cambio propuesto está en negrita y subrayado.	**[188] Procede** Se ajusta la redacción.	**Artículo 14. Responsabilidades sobre la Auditoría Interna o de la función equivalente**
	[189]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 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. En el punto c, puesto que los planes de acción que generalmente	**[189] Procede** Se ajusta la redacción. a. Las recomendaciones de la auditoría externa de TI podrán ser incorporadas o no dentro de los planes de acción para atender los hallazgos identificados, lo anterior, a criterio de la entidad con el fin de mitigar los riesgos que se identifiquen como resultado de la auditoría externa de TI. b. En todo caso, 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	

	se definen después de la auditoría externa de TI son muchos (más de 200), se podría establecer que el alcance sea para aquellos que tienen un nivel de riesgo alto. En particular, la auditoría interna del Banco Popular los evaluará en función de su nivel de riesgo, principalmente para aquellos que tengan un nivel de riesgo alto, considerando valorar si atienden lo recomendado por el auditor externo.	establecidos por la entidad o empresa supervisada. c. Con relación a los hallazgos y su nivel de riesgos, cabe destacar que la matriz de evaluación indica entre otras cosas lo siguiente: Debilidades del proceso: Los profesionales deben documentar el trabajo realizado, registrar la información y evidencia recopilada y documentar cualquier hallazgo identificado relacionado al proceso auditado, se incluye los factores que provocan una posición desfavorable respecto a las actividades del proceso, por ejemplo, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente del proceso. Los hallazgos deben indicar: la condición, criterio, causa, efecto. Cuando corresponda: riesgo y recomendación por cada hallazgo. (Ref. ITAF. 2204.2.2) d. Por lo tanto, la matriz de evaluación no señala una categorización del nivel de riesgos, y la atención de los hallazgos y recomendaciones queda en función del apetito, tolerancia y capacidad de riesgos establecido por la organización en su declaración de apetito de riesgos.	
	[190]FEDEAC Debe ampliarse con más detalle el alcance funcional de la Auditoría Interna como tercera línea de defensa. ¿Los resultados de las revisiones deben ser presentados al Órgano de Dirección? No se señala esa responsabilidad. b) Este plan debe implementarse con base en el alcance definido por el Órgano de Dirección.	**[190] Procede** Se ajusta la redacción con parte de las observaciones, para aclarar las responsabilidades como parte de la tercera línea de defensa. Adicionalmente, el Reglamento de Gobierno Corporativo en el Artículo 25 “Comité de auditoría”, indica entre otras disposiciones que dicho órgano colegiado debe:	

		25.4 Revisar y aprobar el programa anual de trabajo de la auditoría interna o equivalente y el alcance y frecuencia de la auditoría externa, de acuerdo con la normativa vigente.	
	[191]CFBNCR Para los artículos 8,9,10,11,13,14 y 15Se sugiere revisar la pertinencia de algunas responsabilidades establecidas en las secciones II, III y IV, dada la existencia del principio de proporcionalidad. Enel entendido que, en apego a las facultades definidas por ley, el órgano de dirección tiene funciones asociadas principalmente a la aprobación de políticas, el apetito de riesgo, reglamentos, la estrategia de la entidad, asignar responsabilidades y recursos, entre otros y es responsabilidad de la administración activa su ejecución, además de alinear los procesos, procedimientos, registros a los criterios aprobados por el órgano. Dicho lo anterior, se considera que algunas funciones están utilizando verbos descritos en términos de funciones administrativas y operativas que son más bien responsabilidad del Administración, y no del órgano de dirección ni de los comités de apoyo. Por ejemplo, no es competencia del órgano de dirección el aplicar una evaluación, pero sí debe velar porque se establezca, supervisar y conocer los resultados de la evaluación y dimensionar los	**[191] Procede** Se ajustan algunas de las responsabilidades con los infinitivos correspondientes al Órgano de Dirección. Las responsabilidades establecidas en la presente propuesta reglamentaria complementan y refuerzan los mecanismos de control específicos relacionados con cada disposición tutelada en la propuesta.	

	alcances. En ese sentido, se sugiere una revisión integral de los alcances consignados en esas secciones, para una adecuada asignación de responsabilidades, conforme al rol de cada una de las partes y las mejores prácticas. Para efectos de facilitar la aplicación del acuerdo en cuestión, se recomienda que los lineamientos de la gestión de los procesos sobre la seguridad de la información y la seguridad cibernética, evaluación de las necesidades de las partes interesadas y la estrategia para la resiliencia operativa digital estén contenidas en el marco de gobierno y gestión de TI, donde se delimiten las responsabilidades de las partes involucradas en su ejecución. Aplicando esta recomendación, podría generarse un único artículo de responsabilidades que se homologuen o alineen en estructura y alcance a otros reglamentos vigentes como: CONASSIF 4-16, CONASSIF 12-21 y SUGEF 2-10.Respecto a la gestión del comité de TI, también le aplica el principio de proporcionalidad por lo que se sugiere alinear su gestión al artículo 24 del acuerdo CONASSIF 4-16 Reglamento de Gobierno Corporativo y no concentrar sus funciones en aspectos administrativos que son responsabilidad de la Administración, pero sí es responsabilidad de la		

	Administración el rendir cuentas de la gestión de aplicación del marco de gobierno y gestión de TI que incluyan aspectos como resultados de evaluaciones al proceso, ya sean internas o externas, implementación de la estrategia, indicadores de desempeño, entre otros.		
	[192]BCR • En el artículo "14 Responsabilidades sobre la Auditoría Interna o de la función equivalente", o Sobre las funciones detalladas, se solicita que se aclare los alcances de: La actividad "Supervisar el cumplimiento de las políticas y los procedimientos que se establezcan en relación", ya que las Auditorías internas están inhibidas de ejecutar labores de administración como la supervisión. Se sugiere revisar la redacción. o Las actividades de seguimiento sobre los planes de acción para atender los hallazgos que se identifiquen como resultado de la auditoría externa de TI. De tal forma que se aclare si: ¿Se definirá un esquema para ello? ¿Se definirá un instrumento para ejecutar las valoraciones? ¿A quién se debe de reportar los resultados de las valoraciones y con qué periodicidad? ¿Para los resultados de la reciente auditoría externa de TI quién deberá ejecutar el seguimiento de los planes de acción, la Auditoría ¿Interna o la SUGEF? o De parte de la administración consultamos:	**[192] Procede** Se ajusta la redacción con parte de las observaciones, para aclarar las responsabilidades como parte de la tercera línea de defensa.	

	• Visualizando una implementación ágil, ¿La participación de la auditoría interna, se ve como parte del proceso de implementación del plan de acción, en la etapa de verificación de la efectividad del producto final?		
	[193]ISACA Debería definirse la responsabilidad que tiene la Auditoría Interna, la obligatoriedad de contar con Auditor de TI y que las funciones sean separadas de las de otras áreas de control como Control Interno, Contraloría de Servicios, y consultores externos, que también son frecuentes en las entidades supervisadas. En esta función: "a) Supervisar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI." se debería hacer referencia a las TIC, para evitar pensar que TIC es un área. En las entidades la TIC no necesariamente es gestionada por un área especialista para ello; la descentralización ha permitido implementar tecnología fuera de la responsabilidad de los integrantes de áreas de TIC.	**[193] No procede** Las disposiciones se alinean con los aspectos normados en el Acuerdo CONASSIF 4-16. Adicionalmente, el artículo 6 del Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16, indica que el Órgano de Dirección es el responsable de aprobar la estructura organizacional y funcional de la entidad y proporcionar los recursos necesarios para el cumplimiento de sus responsabilidades. Lo anterior implica, entre otros aspectos, que: Constituye y establece 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. Por lo tanto, queda a discreción de la entidad definir contar con un auditor de TI. Por otra parte, la definición de TI para efectos de este reglamento incluye las comunicaciones según e el inciso l del artículo 3 Definiciones.	
En relación con las tecnologías de información, la Auditoría Interna o la función equivalente, al menos, debe:	**[194]COOPEBANPO** No es claro esta definición de responsabilidades en el artículo 13	**[194] No procede** El término equivalente es ampliamente utilizado en el Reglamento de Gobierno	En relación con las tecnologías de información, la Auditoría Interna o la función equivalente, como parte

	se asignan responsabilidades al Comité de TI o función equivalente, en este artículo se le asignan más responsabilidades, pero solo a la función equivalente, pareciera que esto lo tiene que hacer una auditoría interna o la estructura que haya definido la empresa si no tiene comité de ti. De ahí la importancia de definir correctamente que se espera de esa función equivalente al comité de TI.	Corporativo. Equivalente es un adjetivo que expresa algo que tiene igual valor, estimación, potencia o significado. Que supone o implica igualdad o paridad en eficacia, valor, estimación, atribución o categoría. ‖ En cuestiones idiomáticas o de traducción, que significa lo mismo o que son muy parecidos en sus significados. En virtud de lo anterior, las entidades y empresas supervisadas en función del tamaño, complejidad, modelo de negocio y sus riesgos, podrán valorar la asignación de las funciones del comité de TI en una función equivalente, la cual debe cumplir con las responsabilidades asignadas a dicho comité. *Por otra parte se modifica la redacción para mejorar su entendimiento.	de la planificación de los estudios de la auditoría interna y su universo auditable, al menos, debe:
	195]BAC Pregunta ¿Cuál es el ciclo, en años, que debe establecer la auditoría interna en el plan de trabajo para realizar la cobertura completa del marco de gobierno y gestión de TI, de la seguridad de información y seguridad cibernética?	**[195]No procede** Se atiende como consulta. Respuesta: El ITAF de ISACA, así como otras mejores prácticas de auditoría, en relación con la planificación y definición del universo auditable dispone entre otros aspectos, pero no limitado lo siguiente: i. Para valorar correcta y completamente el riesgo relacionado con todo el alcance del área de auditoría de TI, los profesionales deben considerar los elementos siguientes a la hora de desarrollar la planificación de auditoría de TI: 1. Cobertura total de todas las áreas dentro del alcance del universo de auditoría de TI, que incluye el rango de todas las posibles actividades de	

		auditoría y considera la criticidad de sistemas, aplicaciones y procesos 2. Fiabilidad y adecuación de la valoración de riesgos proporcionado por la gerencia 3. Los procesos de la gerencia para supervisar, examinar e informar sobre posibles riesgos o problemas 4. Riesgo de cobertura en actividades relacionadas relevantes a las actividades bajo revisión b. En virtud de lo anterior es responsabilidad de la función de auditoría interna, considerando los riesgos, delimitar el ciclo y ajustar la cantidad de años según su capacidad instalada.	
	[196]CCPA Considerar realizar un cambio en el l inciso a, y sustituir la palabra supervisar, por verificar que está acorde a las funciones que tiene un auditor interno. En el inciso d, es importante mencionar que el accionar del auditor interno es limitado, por lo que se deben de considerar que tipo de trabajos se estarán solicitando por parte de las Superintendencia.	**[196] Procede** Se ajusta la redacción con parte de las observaciones, para aclarar las responsabilidades como parte de la tercera línea de defensa.	
a) Supervisar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.			a) ~~Supervisar~~ Revisar y asegurar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.
b) Implementar un plan de auditoría basado en el riesgo para evaluar la calidad y la eficacia del marco de gobierno y gestión de TI, de la seguridad de la información y de la seguridad cibernética.	**[197]COOPEANDE** 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, con	**[197] Procede** Se ajusta la redacción con parte de las observaciones, para aclarar las responsabilidades como parte de la tercera línea de defensa.	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

	base en el alcance definido por el Órgano de Dirección.		
c)Evaluar la calidad y eficacia de los planes de acción elaborados por la entidad o empresa supervisada que, cuando correspondan, atenderán los hallazgos que se identifiquen como resultado de la auditoría externa de TI.	**[198]ABC** En el inciso c, no resulta claro el sentido de la frase "cuando correspondan", falta precisión si la Auditoría Interna debe evaluar todos los casos cuando se reportan hallazgos, o puede existir un criterio definido por la entidad para determinar cuándo es requerida la validación por parte de la auditoría.	**[198] Procede** Se ajusta redacción.	c)Evaluar la calidad y eficacia de los planes de acción elaborados por la entidad o empresa supervisada que~~,~~ ~~cuando correspondan,~~ atenderán los hallazgos que se identifiquen como resultado de la auditoría externa de TI.
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	**[199]Luis Diego León Barquero** No entiendo la diferencia entre la seguridad de la información y la seguridad cibernética. De hecho, la seguridad cibernética es parte de la seguridad de la información como lo define ISACA en Cybersecurity Fundamentals.	**[199] No procede** La norma ISO 27032 revela que la seguridad cibernética es un subdominio de la seguridad de la información. Adicionalmente, las entidades y empresas supervisadas para su modelo de negocio deben establecer los elementos de control del modelo de líneas defensa, considerando entre otras el principio de proporcionalidad, su tamaño y complejidad, razón por la cual, la propuesta reglamentaria incorpora en el "Artículo 32 Seguridad cibernética" lo siguiente: "Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital. Las entidades y empresas supervisadas deben establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética".	**Artículo 15. Responsabilidades de la unidad o función de gestión de riesgos**
	[200]VIDAPLENA A lo largo de diferentes puntos del Reglamento general de gobierno y	**[200]Procede** Se ajusta la redacción.	

	gestión de la tecnología de la información, acuerdo CONASSIF 5-24 se hace mención o solo utilizan el apetito y tolerancia, pero no consideran el nivel de capacidad en el momento de establecer los niveles de riesgo.		
	[201]CFBNCR Se considera importante incluir o hacer referencia de las responsabilidades que dicta el artículo 15 del presente reglamento, en la norma definida para la gestión de riesgos, acuerdo 2-10, esto con el fin de que las entidades tengan claridad de sus responsabilidades y no medie una dispersión de responsabilidades en materia de gestión de riesgos.	**[201] No procede** En el artículo 95 del Acuerdo SUGEF 2-10 se indica que La entidad, en su gestión del riesgo operativo, debe considerar el riesgo de Tecnologías de Información (TI). Para ello, la Alta Gerencia debe velar que el marco de trabajo de administración de riesgos de TI esté alineado a su proceso de administración de riesgos. Dicho marco de trabajo debe cumplir con los requerimientos dispuestos por el respectivo proceso de conformidad con lo dispuesto en el Acuerdo CONASSIF 5-17. Asimismo, en la actual propuesta de modificación reglamentaria se indica que 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	
	[202]CB Se considera importante incluir o hacer referencia de las responsabilidades que dicta el artículo 15 del presente reglamento, en la norma definida para la gestión de riesgos Acuerdo 2-10, esto con el fin de que las	**[202] No procede** En el artículo 95 del Acuerdo SUGEF 2-10 se indica que La entidad, en su gestión del riesgo operativo, debe considerar el riesgo de Tecnologías de Información (TI). Para ello, la Alta Gerencia debe velar que el marco de trabajo de administración de riesgos de	

	entidades tengan claridad de sus responsabilidades y no medie una dispersión de responsabilidades en materia de gestión de riesgos.	TI esté alineado a su proceso de administración de riesgos. Dicho marco de trabajo debe cumplir con los requerimientos dispuestos por el respectivo proceso de conformidad con lo dispuesto en el Acuerdo CONASSIF 5-17. Asimismo, en la actual propuesta de modificación reglamentaria se indica que 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.	
	[203]SEGUROSLAFISE Valorar la posibilidad de incluir transitorios para este tipo de solicitudes que generan inversión en recursos varios en ajustar las unidades o funciones.	**[203] Procede** Se incluye el transitorio	
	[204]ISACA El título induce a pensar que es un área no tan fuerte como se requiere, ya que indica unidad o función, y esas palabras denotan actividad ad hoc. Al igual que el CISO, la función de gobernar y gestionar riesgos organizacionales corresponde a la alta gerencia.	**[204] No Procede** El artículo 1 de la presente modificación reglamentaria, entre otras disposiciones, 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. Por lo que se mantiene la misma denominación que en dichos marcos regulatorios a fin también de guardar consistencia.	

En relación con las tecnologías de información, la unidad o función de gestión de riesgos, al menos, debe:	**[205]AAP** Valorar la posibilidad de incluir transitorios para este tipo de solicitudes que generan inversión en recursos varios en ajustar las unidades o funciones	**[205] Procede** Se incluye un transitorio.	En relación con las tecnologías de información, la unidad o función de gestión de riesgos, al menos, debe
a) Incorporar la gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética dentro de la gestión de riesgos de la entidad o empresa supervisada.		Se modifica la redacción para mejorar el entendimiento según lo indicado en observaciones.	a) Incorporar la gestión de los riesgos tecnológicos, de tecnologías emergentes, de la seguridad de la información y de la seguridad cibernética dentro de la gestión de riesgos de la entidad o empresa supervisada.
b) Incorporar el apetito de riesgo y la tolerancia de los riesgos tecnológicos, de seguridad de la información y de seguridad cibernética, dentro de la declaración de apetito de riesgo de la entidad o empresa supervisada.		Se modifica la redacción para mejorar el entendimiento según lo indicado en observaciones.	b) Incorporar el apetito de riesgo, ~~y~~ 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.	**[206]FEDEAC** Valorar si los alcances de la función de riesgos deben ser más específicos. c) definir el alcance especifico de los trabajos a solicitar por la superintendencia.	**[206]No procede** Esta disposición tiene como objeto reforzar el trabajo de la función de riesgos como segunda línea de defensa, al solicitar trabajos específicos de acuerdo con el riesgo identificado. En virtud de las facultades que el marco legal otorga al regulador, las Superintendencias podrán establecer las disposiciones que permitan mejorar el ambiente de control interno dentro del modelo de las cuatro líneas de defensa. (1era línea Gestión, 2da línea funciones de control, 3ra línea Auditoría Interna, 4ta línea Auditorías Externas y Supervisores).	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.	**[207]COOPEFYL** Se exime de la aplicación de capítulo a las cooperativas de ahorro y crédito sujetas al Acuerdo Sugef 25-23. Favor revisar los lineamientos generales del anexo 2, ya que están aplicando para efectos de la Auditoría Externa que al menos se tengan procesos de gestión de TI, por tanto, en apariencia hay una contradicción.	**[207]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 "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, al menos, los procesos de evaluación que se especifican en el anexo 2 de los lineamientos generales del presente reglamento.	La gestión de TI de las entidades y empresas supervisadas es tipificada de manera predeterminada como gestión de TI individual.
	[208]BAC Para el caso de la TI tipificada como corporativa ¿Es necesario realizar una nueva solicitud para la	**[208] No procede** El reglamento en la disposición transitoria segunda. Gestión de TI corporativa, indica que los grupos y	

	inclusión de la Corredora de Seguros? Esto considerando que, en el año 2017, cuando se realizó la primera solicitud de tipificación de la TI, se había incluido la Corporación Tenedora BAC Credomatic S.A. como parte de las compañías a las que se les brinda el servicio. BAC Credomatic Corredora de Seguros S.A, es parte del Grupo Financiero BAC Credomatic y de la Corporación Tenedora Bac Credomatic S. A	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. En virtud de lo anterior, si la Sociedad corredora de seguros estaba incluida en la solicitud y fue comunicado su aceptación, no se requiere realizar dicha solicitud.	
	[209]INS Se estima que se le están otorgando al Supervisor facultades que son propias de la administración de las entidades supervisadas, por cuanto en las tres normas, en ese respectivo orden, se faculta al supervisor para requerir: conformación de comité de TI individual, gestiones de TI individuales, así como infraestructuras de almacenamiento diferentes a las adoptadas por las supervisadas.	**[209] No procede** El supervisor tiene la facultad de solicitar cambios si observa una gestión inadecuada dentro de la organización. Los supervisores cumplen un rol de verificar que las operaciones se realicen de manera eficiente y conforme a los estándares establecidos. Cuando identifican problemas o áreas que necesitan mejoras, tienen la responsabilidad de informar y recomendar ajustes o cambios para optimizar el desempeño. En virtud de lo anterior se incluyen en la propuesta disposiciones para la superintendencia y para las entidades, las cuales están en función de sus riesgos, tamaño, complejidad y modelo de negocio.	
	[210]BCR Es necesario aclarar los alcances y las condiciones/criterios bajo los cuales se podría dar esta petición de que puede requerir que se establezca una gestión de TI individual para la respectiva entidad o empresa…, que sería de acatamiento obligatorio, con	**[210] No procede** 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	

	implicaciones estructurales y de costo.	establezca una gestión de TI individual para la respectiva entidad o empresa.	
	[211]ISACA Si existen las condiciones para tipificar la gestión de TI como corporativa, establecidos en los lineamientos generales del presente reglamento, ¿por qué se deja abierta la posibilidad de usar un mismo marco de gobierno y de gestión de TI o no?, tal discrecionalidad se indica en el párrafo anterior.	**[211] No procede** Las entidades y empresas supervisadas son de naturaleza jurídica distinta y dependiendo de su tamaño, complejidad y modelo de negocio, se podrían considerar distintos riesgos, porque sus marcos podrían variar.	
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 como el plazo de respuesta. Las Superintendencias deben coordinar la respuesta a esta solicitud.			La solicitud debe contener una justificación debidamente sustentada que demuestre que se cumplen las condiciones para que la gestión de TI sea tipificada como corporativa. Las condiciones para tipificar la gestión de TI como corporativa están establecidos en los lineamientos generales del presente reglamento, así como el plazo de respuesta. Las Superintendencias deben coordinar la respuesta a esta solicitud.
En el caso que se determine que la gestión de TI corporativa no atiende en forma adecuada y oportuna las funciones y obligaciones indicadas en este reglamento, para alguna de las entidades o empresas que constituyen el grupo o conglomerado, la Superintendencia responsable de la supervisión de dicha entidad o empresa puede requerir que se establezca una gestión de TI individual para la respectiva entidad o empresa.			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			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.			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.	**[212]Luis Diego León Barquero** Es necesario separar las funciones y responsabilidades del órgano de gobierno y la administración. Por lo tanto, la Unidad de TI no debería estar encargado del marco de gobierno. Yo cambiaría el artículo 17 como sigue: 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, y su marco de gestión de TI. El cambio propuesto está en negrita y subrayado.	**[212] No procede** La disposición hace referencia a que la unidad de TI debe apoyar y facilitar la ejecución de los procesos internos. Las responsabilidades de gobierno y gestión están claramente establecidas en las distintas disposiciones del presente reglamento.	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.
	[213]MUCAP En las Responsabilidades de la Alta Gerencia, se indica “Designar las áreas de negocio y de TI responsables de implementar el marco de gobierno y de gestión TI.” No obstante, este artículo limita a una sola Unidad de TI, encargada de implementar las soluciones tecnológicas del marco de gestión. Lo que hace que no quede claro la responsabilidad cuando varias áreas de la entidad realizan funciones de TI. Adicionalmente, se debe considerar que el marco de gobierno y gestión de TI involucra diferentes unidades organizacionales (proveedores,	**[213] No procede** El término “unidad de TI” hace referencia al área o unidad funcional que gestiona las TI en la organización y esta a su vez podrá estar conformada por otras subáreas que podrán apoyar y facilitar la ejecución de los procesos internos de la organización, así como los procesos de TI que sean de naturaleza técnica. Con relación a la responsabilidad de la Alta Gerencia, que indica “Designar las áreas de negocio y de TI responsables de implementar el marco de gobierno y de gestión TI.”, esta disposición se establece ya que 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,	

	talento humano, procesos, etc.), no solo las áreas de TI.	auditoria, control, seguridad de la información, recursos humanos, gestión de calidad, gestión de proveedores, entre otros. En virtud de lo anterior, la unidad de TI se encarga de apoyar y facilitar las soluciones tecnológicas y de naturaleza técnica y el marco de gobierno y gestión de TI dispone los procesos que según el modelo de negocio pueden ser ejecutados de forma transversal o por la unidad de TI.	
	[214]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 y no sólo de TI.	**[214] No procede** El reglamento utiliza una terminología que está con consonancia con el resto de la normativa emitida 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.	
	[215]CFBNCR Se sugiere modificar de la siguiente manera: "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	**[215] No procede** Se modificó el artículo 34 sobre unidades y funciones organizacionales para aclarar la redacción,	

	los procesos internos, así como su marco de gobierno y gestión de TI, tomando en consideración la seguridad de la información"		
	[216]ABC Se sugiere adicionar al final del artículo la frase: "tomando en consideración la seguridad de la información."	**[216] No procede** Se modificó el artículo 34 sobre unidades y funciones organizacionales para aclarar la redacción,	
	[217]CB Se sugiere modificar de la siguiente manera: "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, tomando en consideración la seguridad de la información."	**[217] No procede** Se modificó el artículo 34 sobre unidades y funciones organizacionales para aclarar la redacción,	
	[218]ISACA Nuevamente la palabra unidad y función equivalente, no es consistente con la realidad. Las entidades y empresas del SFN tienen gerencias o direcciones de TI, no unidades, precisamente el CTIO pertenece a la Alta Gerencia, lo mismo sucede con el CISO. Desde el concepto de unidad es muy difícil implementar estrategias de gobierno.	**[218] No procede.** En el artículo 34 de la presente propuesta, se establece que las entidades y empresas supervisadas deben establecer unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen los riesgos de la seguridad cibernética. Por su parte, como respuesta a las observaciones 215,216, y 217 se incorporan la seguridad de la información.	
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:	**[219]BPDC** 1-En el punto a) parece haber un problema de redacción, pues parece indicar que le corresponde	**[219] Procede** Se ajusta la redacción considerando parte de las observaciones.	La Unidad de TI o la función equivalente es responsable de:

	a la unidad de TI ejecutar las acciones del marco de gobierno de la entidad supervisada. Aunque el mismo reglamento establece otros involucrados (Riesgos, Planificación, Proveeduría, Auditoría, etc). ¿Se entiende que se refiere a ejecutar las actividades asignadas a la unidad de TI dentro del marco? 2-En el punto b, considerar que hay riesgos tecnológicos que no están bajo la directa supervisión o capacidad de gestión de la unidad de TI, por ejemplo, la capacitación del personal de la institución en operación y manejo de herramientas de TI. Nuevamente se entendería que la responsabilidad se limita a los riesgos asignados a la unidad de TI. 3-En el punto c, considerar que la estrategia de TI corresponde al Órgano Director o en su defecto al Comité. La unidad de TI puede no contar con las capacidades suficientes para hacer planificación estratégica especialmente si su rol dentro de la empresa es funcional o de soporte (no le reporta a la alta dirección).	Esta disposición hace referencia directa a la unidad de TI, por consiguiente, la gestión de los riesgos estaría circunscrito en dicho ámbito. Cabe destacar que el "Artículo 1. Objeto", entre otras disposiciones establece 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. En cuyo caso se espera que las entidades y empresas supervisadas en función de su tamaño, complejidad, modelo de negocio establezcan una gestión integral de riesgos. Se elimina el inciso "c) Implementar y ejecutar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada."	
	[220]MUCAP 1) Las acciones del marco de gobierno y gestión de TI también son ejecutadas por otras áreas de negocio. 2) Se delimita "proyectos relacionados con TI", sin embargo, no existe claridad lo que	**[220] Procede** Se ajusta la redacción considerando los puntos 1 y 4 de las observaciones. Respectos a los demás puntos de las observaciones, se considera que no aplican para realizar ajustes a la disposición reglamentaria.	

	sucede con los proyectos que tienen componentes tecnológicos y que no están a cargo de la Unidad de TI. Esto debido a que, en la mayoría de los proyectos, la función de TI es un habilitador; sin embargo, la responsabilidad de implementación es de otras áreas de negocio. 3) La arquitectura tecnológica es solo una parte del modelo de arquitectura de la entidad, por lo tanto, esta responsabilidad no debería ser de la unidad de TI. 4) En muchos casos, las áreas de negocio son las responsables de los bienes o servicios de TI contratados, siendo el Administrador del Contrato de las áreas correspondientes, las encargadas de velar por el cumplimiento contractual.	1-Se modifica como parte de la observación [219 - a] 2-Las entidades y empresas supervisadas deben establecer métodos de administración de proyectos acorde a su tamaño, complejidad y modelo de negocio, en donde se gestionen aspectos como alcance, costos, riesgos, partes interesadas, entre otros. En virtud de lo anterior las unidades gestoras de proyectos de cada entidad o empresa supervisada deberán involucrar a la unidad de TI como parte interesada cuando el proyecto de negocio tenga componentes de TI. 3-Se ajusta según TOGAF. 4-Se elimina la disposición h, ya que está contenida en términos generales dentro de lo dispuesto en el artículo 29.	
	[221]COOPEALIANZA Se solicita la siguiente redacción: a) Ejecutar las acciones del marco de gobierno y gestión empresarial que le corresponden. Desarrollar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada. c) Desarrollar la planificación y la estrategia de TI, o integrar la estrategia de TI con la estrategia organizacional, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada.	**[221] No Procede.** Se atiende con parte de la observación 219.	
	[222]VIDAPLENA	**[222] Procede**	

	A lo largo de diferentes puntos del Reglamento general de gobierno y gestión de la tecnología de la información, acuerdo CONASSIF 5-24 se hace mención o solo utilizan el apetito y tolerancia, pero no consideran el nivel de capacidad en el momento de establecer los niveles de riesgo.	Se ajusta la redacción.	
	[223]BCR 1-Inciso a. Conforme se asignan los procesos del marco de gobierno y gestión de TI, se encuentran distribuidos a lo largo de la Entidad, por lo que la ejecución de las acciones de dicho marco, no son completamente del ámbito de responsabilidad de la unidad de TI. Se recomienda cambiar la redacción para poder abarcar todas las áreas que ejecutan las acciones del marco de gobierno y gestión de TI. 2-Inciso f. Aclarar si se hace referencia a un modelo de Arquitectura de TI o de Arquitectura Empresarial. 3- Inciso e): "Asegurar que la gestión de los datos de la entidad o empresa supervisada se realice de manera efectiva y eficiente, atendiendo, en función de sus riesgos, las necesidades de confidencialidad, integridad, disponibilidad, no repudio y auditabilidad.", las cuales salen de la cobertura de una Unidad de TI en los términos definidos, por lo que se hace importante que se aclare los alcances de esta responsabilidad.	**[223]No Procede** 1-Inciso a- Se ajusta la redacción considerando parte de las observaciones. Esta disposición hace referencia directa a la unidad de TI, por consiguiente, la gestión de los riesgos estaría circunscrito en dicho ámbito. Cabe destacar que el "Artículo 1. Objeto", entre otras disposiciones establece 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. En cuyo caso se espera que las entidades y empresas supervisadas en función de su tamaño, complejidad, modelo de negocio establezcan una gestión integral de riesgos. 2- Se ajusta según TOGAF. 3-Inciso e- Se mueve a las responsabilidades de la Alta Gerencia considerando el modelo de Arquitectura de TOGAF. Los puntos señalados en las observaciones que no tienen numeración se atienden de conformidad con lo	

	• De igual forma para el inciso h) "Verificar el cumplimiento contractual por parte de los proveedores cuando se les delegan bienes o servicios de TI", ya que los bienes y servicios adquiridos en la organización no son hechos únicamente por la Unidad de TI e inciso i). • Las funciones indicadas son de todos los responsables de Gobernar y Gestionar TI. Sugerir cambiar el título del Artículo. • Se solicita valorar el ajuste a la redacción actual; lo anterior para que no se mal interprete por el resto de la organización que este reglamento es solo responsabilidad de la unidad de TI ya que para su definición, normalización, implementación y ejecución existe dependencia de muchas áreas fuera de la unidad organizacional de TI, y que soportan procesos especializados como lo son: la gestión del Gobierno Corporativo, la gestión de Riesgos, la gestión de Proyectos, la gestión de Datos, la gestión de Arquitectura Empresarial, la gestión de Activos, la gestión de Costos, la formulación y gestión de Contratos.	ajustado a partir de las observaciones [220] y [223].	
	[224]ISACA Inciso f: se refiere a la arquitectura tecnológica o empresarial? Inciso h: Recomendaría que se vea como terceros en general no sólo proveedores, ya que garantizar una adecuada gestión de riesgos de	**[224] Procede** Se ajustó la redacción. Por otra parte, importante señalar que se elimina el inciso h, ya que está contenida en términos generales dentro de lo dispuesto en el artículo 29.	

	seguridad de la información, seguridad cibernética o continuidad podría tener relación con otros tipos de terceros que consumen información de la organización para su labor como lo es el supervisor por ejemplo y allí el intercambio de información y otros también debe garantizarse por medios seguros, privados y disponibles.		
a) Ejecutar las acciones del marco de gobierno y gestión de TI que le correspondan a la entidad o empresa supervisada.	**[225]POPULARPENSIONES** 1-La redacción del inciso a) indica que es la unidad de TI es la responsable de ejecutar las acciones del marco en su totalidad, siendo que el Marco de Gobierno y Gestión excede en mucho a la unidad de TI, incluye actividades por ejemplo para las unidades de Riesgo, Capital Humano, Gerencia, Control Interno, Proveeduría, Presupuesto, entre otros. En lo relativo al inciso 2-b) los riesgos tecnológicos son una categoría de riesgo lo cual no implica que su gestión y responsabilidad sea necesariamente asignada a la unidad de TI. No todos los riesgos tecnológicos son asignados a la Unidad de TI, por lo cual se considera necesario modificar este inciso paraque indique los riesgos tecnológicos asignados a la Unidad de TI.	**[225]Procede** 1-Se ajusta la redacción. 2-Se elimina el inciso b, ya que está contenido en el artículo 15.	a) Ejecutar ~~las acciones~~s las estrategias para la implementación del marco de gobierno y gestión de TI ~~que le correspondan a la entidad o empresa supervisada~~.
	[226]CB Es importante aclarar que el mismo Reglamento establece que las acciones del marco de gobierno y gestión de TI también son	**[226] Procede** Se ajusta la redacción con parte de las observaciones [219].	

	ejecutadas por otras áreas de negocio (Riesgos, Auditoría, Planificación, etc.) por lo que es importante revisar la redacción de este inciso, pues pareciera que solo asignan las responsabilidades a TI, de tal forma que debe ajustarse su redacción.		
b) Gestionar los riesgos tecnológicos de conformidad con el apetito y la tolerancia del riesgo de la entidad o empresa supervisada.	**[227]CATHAY** Gestionar los riesgos tecnológicos de conformidad con el apetito y la tolerancia del riesgo de la entidad o empresa supervisada. Hay riesgos tecnológicos que no están bajo la directa supervisión o capacidad de gestión de la unidad de TI, por ejemplo, la capacitación del personal de la institución en operación y manejo de herramientas de TI. Nuevamente se entendería que la responsabilidad se limita a los riesgos asignados a la unidad de TI. Desarrollar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada. La estrategia de TI corresponde al Órgano director o en su defecto al Comité. La unidad de TI puede no contar con las capacidades suficientes para hacer planificación estratégica especialmente si su rol dentro de la empresa es funcional o de soporte (no le reporta a la alta dirección), se podría revalidar la redacción para su mejor comprensión.	**[227] Procede** Se elimina el inciso b, ya que está contenido en el artículo 15.	~~b) Gestionar los riesgos tecnológicos de conformidad con el apetito y la tolerancia del riesgo de la entidad o empresa supervisada.~~ b)Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos establecidos.
c)Desarrollar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos	**[228]Luis Diego León Barquero**	**[228] Procede**	~~c)Desarrollar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos~~

estratégicos establecidos por la entidad o empresa supervisada.	Es necesario separar las funciones y responsabilidades del órgano de gobierno y la administración. Por lo tanto, la Unidad de TI no debería estar encargado del marco de gobierno. Yo cambiaría el inciso a del artículo 18 como sigue: a) Ejecutar las acciones del marco de gobierno y gestión de TI que le correspondan a la entidad o empresa supervisada. El cambio propuesto está en negrita, tachado y subrayado.	Se atiende como parte de la observación [219]. Se elimina el inciso "c) Implementar y ejecutar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada."	~~estratégicos establecidos por la entidad o empresa supervisada.~~ c) Diseñar e implementar la arquitectura tecnológica y de aplicaciones alineada a la arquitectura de negocio y a la arquitectura de información, a fin de soportar las operaciones de la entidad o empresa supervisada.
d)Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos acordados.		Se modifica la redacción para mejorar el entendimiento según lo indicado en observaciones.	d)~~Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos acordados.~~ 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 la gestión de los datos de la entidad o empresa supervisada se realice de manera efectiva y eficiente, atendiendo, en función de sus riesgos, las necesidades de confidencialidad, integridad, disponibilidad, no repudio y auditabilidad.		Se modifica la redacción para mejorar el entendimiento según lo indicado en observaciones.	~~e) Asegurar que la gestión de los datos de la entidad o empresa supervisada se realice de manera efectiva y eficiente, atendiendo, en función de sus riesgos, las necesidades de confidencialidad, integridad, disponibilidad, no repudio y auditabilidad.~~ 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) Diseñar un modelo de arquitectura para soportar las operaciones de la entidad o empresa supervisada.	**[229]CFBNCR** 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".	**[229] No procede** Se ajusta la redacción considerando lo establecido en The Open Group Architecture Framework (TOGAF).	~~f) Diseñar un modelo de arquitectura para soportar las operaciones de la entidad o empresa supervisada.~~ 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.
	[230]ABC Se sugiere modificar la redacción 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”.	**[230] No procede** Se ajusta la redacción considerando lo establecido en The Open Group Architecture Framework (TOGAF).	
	[231]OPC-CCSS En el punto f) de este apartado se indica que una de las responsabilidades de la Unidad de TI o de la función equivalente es "Diseñar un modelo de arquitectura para 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 aplicaría. Por lo tanto, se sugiere cambiar la redacción o valorar si se elimina.	**[231] No procede** Se ajusta la redacción considerando lo establecido en The Open Group Architecture Framework (TOGAF).	
g) Establecer los controles para el desarrollo del ciclo de vida de los servicios y de los sistemas de información, los cuales aseguren la confidencialidad, integridad, disponibilidad, calidad, mantenimiento y los cambios por excepción o de emergencia.		Se eliminó el párrafo de conformidad con las observaciones y para mejorar el alcance de las disposiciones.	~~g) Establecer los controles para el desarrollo del ciclo de vida de los servicios y de los sistemas de información, los cuales aseguren la confidencialidad, integridad, disponibilidad, calidad, mantenimiento y los cambios por excepción o de emergencia.~~
h) Verificar el cumplimiento contractual por parte de los proveedores cuando se les delegan bienes o servicios de TI.		Se eliminó el párrafo de conformidad con las observaciones y para mejorar el alcance de las disposiciones.	~~h) Verificar el cumplimiento contractual por parte de los proveedores cuando se les delegan bienes o servicios de TI.~~
i)Asegurar que los bienes y servicios de TI críticos estén identificados, sean gestionados de manera efectiva y eficiente, y se mantengan disponibles.		Se eliminó el párrafo de conformidad con las observaciones y para mejorar el alcance de las disposiciones.	~~i)Asegurar que los bienes y servicios de TI críticos estén identificados, sean gestionados de manera efectiva y eficiente, y se mantengan disponibles.~~

j) Asegurar que los requerimientos de las entidades y empresas supervisadas sean atendidos de manera equitativa y en función de los riesgos de cada negocio cuando la gestión de TI es corporativa.	**[232]CAJAANDE** J. Favor ampliarnos ¿Qué documentación se consideraría probatoria de esta acción?	**[232] No Procede** Se elimina el inciso j). Se eliminó el párrafo de conformidad con las observaciones y para mejorar el alcance de las disposiciones.	~~j) Asegurar que los requerimientos de las entidades y empresas supervisadas sean atendidos de manera equitativa y en función de los riesgos de cada negocio cuando la gestión de TI es corporativa.~~
Sección II. Tratamiento de datos, activos de información, aplicaciones, sistemas de información y soluciones tecnológicas			**Sección II. Tratamiento de datos, activos de información, aplicaciones, sistemas de información y soluciones tecnológicas**
Artículo 19. Clasificación de activos de información, del impacto en caso de presentarse una brecha de seguridad de la información y del acceso y uso de los datos		Se modifica la redacción y se traslada lo referente a brechas al capítulo IV**.**	**Artículo 19. Clasificación de activos de información~~, del impacto en caso de presentarse una brecha de seguridad de la información~~ y del acceso y uso de los datos**
Las entidades y empresas supervisadas deben clasificar sus activos de información, el impacto potencial en caso de presentarse una brecha de seguridad de la información, así como el acceso y uso de los datos y los activos de información de conformidad con el modelo de clasificación establecido en los lineamientos generales del presente reglamento.	**[233]Luis Diego León Barquero** No entiendo la redacción sobre la clasificación de los datos, pues no se refiere a un modelo de criticidad.	**[233] Procede** Se modifica el texto de la disposición para mejorar el entendimiento.	Las entidades y empresas supervisadas deben clasificar sus activos de información~~, el impacto potencial en caso de presentarse una brecha de seguridad de la información, así como el acceso y uso de los datos y los activos de información~~ de conformidad con el modelo de clasificación establecido en los lineamientos generales del presente reglamento.
	234]BPDC ¿No queda clara esta responsabilidad dentro de la institución, a quién se le asigna?	**[234] No procede** La entidad es la encargada de definir quién es el responsable de clasificar y etiquetar los activos de información y los datos.	
	[235]MUCAP 1) No existe claridad con lo indicado en la redacción, ya que el verbo principal es "deben clasificar", lo cual no permite comprender a qué hace alusión con clasificar el acceso y uso de los datos. 2) No existe claridad si esto implica cambios en el Perfil Tecnológico, así como no existe una indicación escritita en qué año se debería estar reportando.	**[235 - 1] Procede** 1-Se modifica el texto de la disposición para mejorar el entendimiento. 2-Se aclara en los lineamientos los temas del perfil de TI, además, se incorporó un transitorio para el perfil de TI.	
	[236]AAP	**[236] No Procede**	

	Se sugiere que se permita que cada compañía defina sus propias clasificaciones de la manera que mejor se ajuste a sus propios escenarios, no solo para los activos si no las distintas clasificaciones citadas en los lineamientos, se considera que definir clasificaciones que todas las compañías deben acatar va en detrimento de la forma en que cada compañía decide operar y administrar. Favor no obligar a los supervisados a las clasificaciones sugeridas o definir transitorios.	Los lineamientos de la presente propuesta de modificación reglamentaria contienen las pautas relevantes para las Superintendencias que buscan homologar los criterios a nivel de todo el sistema financiero costarricense. El contenido de los lineamientos está alineado a los estándares, mejores prácticas y marcos de referencia internacionales, implementados comúnmente por la industria de las tecnologías de información. Adicionalmente, se incluye un transitorio para la identificación de brechas y la implementación de las disposiciones reglamentarias.	
	[237]ABC Se recomienda limitar el alcance a los procesos críticos definidos e identificados por la entidad bancaria.	**[237] No procede** La confidencialidad de los datos está relacionada con cualquier información de la cual es dueña la organización, de manera que, si se evidencia el acceso a los datos para una finalidad distinta a la requerida, su uso sería ilegítimo, incorrecto y la conducta, además de conllevar a consecuencias penales, civiles y disciplinarias, generaría secuelas administrativas. Por lo tanto, al ser un tema de confidencialidad de datos, la clasificación y etiquetado no podría ir en función solamente de la criticidad de un proceso.	
	[238]CB Sobre al artículo 19 y la Sección II de los Lineamientos Generales (Clasificación de Activos de Información), debemos señalar que resulta confusa la clasificación contenida en la sección II de los Lineamientos, pues no existe consistencia entre los criterios de	**[238] Procede** Se modifica el texto para mejorar el entendimiento de la disposición.	

	clasificación propuestos en dicha sección y los criterios propuestos para efectos de calificar un incidente de seguridad que afecte o comprometa los datos, contenidos en la sección VII.2.Se solicita aclarar la diferencia entre los criterios o si sirven propósitos distintos y aclarar que para efectos de notificar incidentes de seguridad solo deben tomarse en cuenta los criterios de la sección VII.2 (Ver Capítulo IV, Sección II). Lo anterior para mayor claridad y seguridad jurídica.		
	[239]SEGUROSLAFISE Favor permitir que cada compañía defina sus propias clasificaciones de la manera que mejor se ajuste a sus propios escenarios, no solo para los activos si no las distintas clasificaciones citadas en los lineamientos, se considera que definir clasificaciones que todas las compañías deben acatar va en detrimento de la forma en que cada compañía decide operar y administrar. Favor no obligar a los supervisados a las clasificaciones sugeridas o definir transitorios.	**[239] No Procede** Los lineamientos de la presente propuesta de modificación reglamentaria contienen las pautas relevantes para las Superintendencias que buscan homologar los criterios a nivel de todo el sistema financiero costarricense**.** El contenido de los lineamientos está alineado a los estándares, mejores prácticas y marcos de referencia internacionales, implementados comúnmente por la industria de las tecnologías de información. Adicionalmente, se incluye un transitorio para identificación de brechas y la implementación de las disposiciones del reglamento.	
	[240]COOPENAE (Impacto Alto, Esfuerzo Medio) Solicita la implementación de un proceso que, para algunas entidades significa volver a desarrollar lo que existía con el lineamiento de COBIT, pues establece requerimientos	**[240] No procede** Las entidades deben identificar sus brechas con relación a las disposiciones establecidas en la presente propuesta de modificación reglamentaria a fin de establecer las acciones requeridas para solventar dichas brechas.	

	puntuales que no eran necesarios en el proceso COBIT.		
	[241]BCR 1• Definir que son activos de información primarios y que son activos de información de apoyo. 2• ¿Se va a incluir en el perfil tecnológico la estructura para clasificar los activos de información en primarios y de apoyo?	**[241] No procede** 1-En los lineamientos se indican los tipos de activos a saber: Activos primarios o activos de información: i. Incluyen la información, los procesos o las actividades de los procesos de la entidad o empresa supervisada. ii. Estos se revelan en el perfil tecnológico a través de los formularios activos de información y procesos de negocio. Activos de soporte de los activos primarios o activos de información: i. Incluyen al menos: hardware, software, dispositivos de redes, personas, estructura organizacional, ubicaciones físicas, entre otros. ii. Estos se revelan en el perfil tecnológico a través de los formularios Equipos, Sistemas de Información, Software, Centros de datos, Bases de datos, Documentos, entre otros. 2-Por otra parte, se actualiza el lineamiento con relación a los temas del perfil de TI y los activos de información, lo cual, atiende el punto 2 de la observación.	
	[242]CCPA Nuestra recomendación es realizar una aclaración sobre los aspectos que debe tomar la administración para la clasificación.	**[242] Procede** Se modifica el texto de la disposición para mejorar la redacción y entendimiento de la propuesta.	
	[243]ISACA La clasificación de la información sigue siendo algo que se relega año a año, y se sustenta que para aplicarla dicha clasificación se requiere de tiempo y presupuesto,	**[243] No procede** El propósito de la disposición busca mitigar los riesgos del comentario.	

	pero no existe una supervisión puntual por parte del CONASSIF. Existen procesos maestros como la Clasificación de la Información que se compone de varios procesos del Modelo COBIT. Estos procesos deben ser implementados de primero, se debe indicar el orden de prioridad para todas las entidades y empresas fiscalizadas. Otros procesos maestros son: SGSI, SGCN, Gestión de Cambios, entre otros. Por otro lado, cuando se implementa esta función, se hace con respecto a la información crítica, referente a la continuidad de las operaciones del negocio, donde debe ser claro y explícito que hasta la información administrativa o de uso interno, son categorías que deben ser protegidas porque existen otros riesgos aparte de la fuga o robo de información, como lo son el sabotaje o el chantaje.		
		Se incluyó párrafo para mejorar el entendimiento del artículo.	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 apoyo deben ser revelados en el perfil tecnológico.	**[244]CAJAANDE** Respetuosamente les agradecemos que nos indique si los ¿Activos de información primarios se refiere a los críticos?	**[244] No procede** En los lineamientos se indican los tipos de activos a saber: Activos primarios o activos de información: i. Incluyen la información, los procesos o las actividades de los procesos de la entidad o empresa supervisada.	Los activos de información primarios y de soporte ~~apoyo~~ deben ser revelados en el perfil tecnológico de conformidad con lo establecido en los lineamientos generales del presente reglamento.

		ii. Estos se revelan en el perfil tecnológico a través de los formularios activos de información y procesos de negocio. Activos de soporte de los activos primarios o activos de información: i. Incluyen al menos: hardware, software, dispositivos de redes, personas, estructura organizacional, ubicaciones físicas, entre otros. ii. Estos se revelan en el perfil tecnológico a través de los formularios Equipos, Sistemas de Información, Software, Centros de datos, Bases de datos, Documentos, entre otros. *****Por otra parte, se modifica la redacción para un mejor entendimiento de la disposición.	
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 bases de datos actualizadas, las aplicaciones, los sistemas de información y las soluciones tecnológicas vigentes que procesan o dan acceso a las bases de datos de las entidades o empresas supervisadas deben estar disponibles y accesibles a las Superintendencias para sus labores de supervisión, sin ningún tipo de restricción o condición.	**[245]BPDC** Se debe especificar que se entiende por un acceso sin ningún tipo de restricción o condiciones a las labores de supervisión. 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 ley 9048. Además, se debe tomar en cuenta los contratos de adhesión que no pueden ser modificados.	**[245] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	~~Las bases de datos actualizadas, las aplicaciones, los sistemas de información y las soluciones tecnológicas vigentes que procesan o dan acceso a las bases de datos de las entidades o empresas supervisadas deben estar disponibles y accesibles a las Superintendencias~~ 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.
	[246]MUCAP Al hacer alusión en términos generales, no queda claro si se refieren a todas las bases de datos o solo a las de los sistemas críticos. Quedando la inquietud también, si	**[246] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	

	es solo de aplicabilidad a los ambientes de producción o también para ambientes de pruebas que existan en la entidad.		
	[247]COOPEANDE A nivel de aplicaciones, sistemas de información y soluciones tecnológicas como servicio (contratos de suscripción y/o adhesión) donde la entidad recibe un servicio con base en criterios pactados a nivel contratos estándar, es importante valorar que la información que sea requerida por la Superintendencia debe ajustarse políticas y procesos que poseen dichos fabricantes para su entrega. Es complejo que fabricantes de clase mundial hagan ajustes a contratos estándar para solicitudes puntuales. Los Fabricantes poseen informes con base en las buenas prácticas y lo que se pretende dejar con más claridad es que la Superintendencia estaría en caso de ser necesario solicitando la información y estando conforme en la forma en que el fabricante la brinda. Lo indicado en el artículo "Las bases de datos deben estar disponibles...y accesibles a las Superintendencias para sus labores de supervisión, sin ningún tipo de restricción o condición." Por lo anteriormente expuesto no es viable que el supervisor tenga acceso a bases de datos sin ninguna restricción o condición, más aún en la infraestructura en la	**[247] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	

	nube donde se cuenta con legislación múltiple.		
	[248]JUPEMA ¿Con qué fin se compartirían las bases de datos? ¿Qué medidas de seguridad tendrá el ente regulador para acceder a las bases de datos? En caso de que se vea vulnerado el acceso por acciones propias del ente regulador, ¿quién asume la responsabilidad? ¿Qué rol requieren para el ingreso a la base de datos? Surge una inquietud sobre la legalidad en brindar acceso total a la base de datos.	**[248] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[249]FEDEAC ¿cuál es el fundamento legal para que la superintendencia tenga acceso irrestricto y sin condición a bases de datos? Cuando las entidades han pactado contratos estándar con proveedores o fabricantes de clase mundial y a nivel internacional, la Superintendencia debe ajustarse a las políticas y procesos que poseen dichos fabricantes para su entrega de información. No es viable que el supervisor tenga acceso a bases de datos sin ninguna restricción o condición, más aún en la infraestructura en la nube donde se cuenta con legislación múltiple. En el acceso de bases de datos por parte del supervisor qué medidas de seguridad tendrá el ente regulador para accederlas y cómo asume su responsabilidad si tales bases de datos son vulneradas producto de su acceso.	**[249] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[250]AAP	**[250] Procede**	

	Propuesta: El entregar acceso a las bases de datos o dar información de clientes es un riesgo, SUGESE debe establecer controles para resguardar la información y asegurar la protección de los mismos una vez le sean suministrados. Los solicitantes de información deben establecer controles de confidencialidad y resguardo de la información, a manera de contrato al igual que a los terceros. Se sugiere eliminar del párrafo la frase "sin ningún tipo de restricción o condición" y colocar de acuerdo con los controles/condiciones que la entidad Supervisada logre exponer para dichas consultas o accesos.	Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[251]COOPEALIANZA Con respecto a la redacción "Asimismo, la plataforma tecnológica donde se procesen estas bases de datos solo puede ser utilizada por las entidades y empresas integrantes del grupo o conglomerado financiero" va en contra de las economías de escala, los servicios en la nube; por lo tanto, se solicita la siguiente redacción más razonable a los tiempos actuales. "Asimismo, la plataforma tecnológica donde se procesan estas bases de datos debe contar con el modelo de responsabilidades compartidas para proteger la infraestructura en la que se ejecutan los servicios que se ofrecen."	**[251] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[252]VIDAPLENA Pregunta	**[252] Procede**	

	¿Como va a funcionar el tema del acceso a las bases de datos? ¿Qué tipo (lectura/ escritura/ acceso total) de acceso se les debe bridar a las superintendencias? También es importante que aclaren o definan el término de lo señalado en el primer párrafo “sin ningún tipo de restricción o condición.”, en cuanto al acceso irrestricto al Ente Supervisor. Cuando la información que se resguarda de los afiliados no es de dominio público y ya hay jurisprudencia sobre ese tema; adicional a que cada empresa también define de acuerdo con las mejores o sanas prácticas, que información es catalogada o clasificada como confidencial; así como la información relacionada con sus clientes se resguarda de la competencia, dado el tipo de negocio en la cual está inmersa la empresa.	Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[253]OPC-CCSS 1. Se sugiere especificar de qué forma será el acceso a las bases de datos por parte de las Superintendencias y el tratamiento que se dará a estas, debido a lo delicado que puede convertirse este tema.2. Según la sesión de trabajo que se tuvo, es necesario que se aclare la intención del regulador respecto a la redacción del punto dado que la redacción da a entender que el acceso debe ser directo a los funcionarios de las superintendencias y según lo	**[253] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	

	explicado esa no es la necesidad del regulador.		
	[254]CB Preocupa que esta disposición establece que se debe dar un acceso irrestricto al supervisor, pues esto implicaría incluso poder hacer modificaciones en las bases de datos. Es claro que la función es de supervisión, pero si se da acceso irrestricto el personal de la superintendencia podría voluntaria o involuntariamente hacer modificaciones en los datos de la institución. En tal sentido, mantener un acceso "sin restricciones ni condiciones" a las Superintendencias a todas las bases de datos, sistemas y aplicaciones del Banco, compromete seriamente la seguridad de la información y la protección de datos personales, materia sobre la que existiría reserva de ley. Se recomienda al Regulador una modificación para que el Reglamento permita condicionar el acceso por parte de las Superintendencias, a las medidas razonables de seguridad y control de acceso con salvaguarda de la protección de datos personales, necesarias para evitar precisamente accesos o usos no autorizados por parte de funcionarios de las Superintendencias. Por lo tanto, el acceso podría ser de lectura total, pero sin derecho a escribir/sobrescribir. En ese orden de ideas, se solicita revisar esta	**[254] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	

	disposición y realizarlas aclaraciones necesarias.		
	[255]SEGUROSLAFISE Propuesta: El entregar acceso a las bases de datos o dar información de clientes es un riesgo, SUGESE debe establecer controles para resguardar la información y asegurar la protección de los mismos una vez le sean suministrados. Los solicitantes de información deben establecer controles de confidencialidad y resguardo de la información, a manera de contrato al igual que a los terceros. Proponemos eliminar del párrafo la frase "sin ningún tipo de restricción o condición" y colocar de acuerdo con los controles/condiciones que la entidad supervisada logre exponer para dichas consultas o accesos.	**[255] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[256]BCR • "Asimismo, la plataforma tecnológica donde se procesen estas bases de datos solo puede ser utilizada por las entidades y empresas integrantes del grupo o conglomerado financiero". Esto no es posible garantizarlo en un ambiente de nube. • Se solicita clarificar o ajustar la redacción ya que la información no debe estar disponible o accesible sin ningún tipo de restricción o condición – debe existir un proceso de gobierno y gestión alineado con otras leyes y reglamentos que defina y asegure los controles y registros documentales mínimos para su	**[256] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	

	acceso y uso (protección de los datos); es requerido no abrir portillos de seguridad. • Se solicita clarificar este alcance en caso de servicios tercerizados. • Se solicita clarificar como se requiere la accesibilidad a las bases de datos. Si es acceso en línea o por petición puntual, lo anterior implica diferentes impactos.		
	[257]ISTMO En los lineamientos generales deben de formularse los procedimientos y los mecanismos de como operará este artículo y dejar claros bajo qué condiciones tendrán los accesos.	**[257] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
	[258]ISACA Con el propósito de evitar que esto se entienda como una "conectividad directa" a los datos de una base de datos y que esto le traslade al supervisor u organismo auditor responsabilidades en cuanto a la aplicación y efectividad de controles que garanticen la seguridad o privacidad de los datos en dicha conectividad, se podría mejorar la redacción para indicar "...deben garantizar la disposición y el acceso a la información requerida por las Superintendencias para poder ejercer sus labores de supervisión, sin ningún tipo de restricción o condición requerida."	**[258] Procede** Se ajusta la redacción considerando parte de las observaciones y de conformidad con las recomendaciones de los principales proveedores de servicios de computación en la nube.	
Cuando existan bases de datos compartidas debe efectuarse una separación del registro de las operaciones de cada entidad y empresa integrante del grupo o conglomerado financiero. Asimismo, la plataforma	**[259]BAC** Se puede aclarar qué se entiende por "separación de los registros de cada entidad", para el caso de que	**[259]No procede** La separación de registros de cada entidad hace referencia a que la entidad o empresa supervisada debe garantizar	Cuando existan bases de datos compartidas entres las entidades y empresas integrantes del grupo o conglomerado financiero, debe efectuarse una separación del registro de las operaciones de cada

tecnológica donde se procesen estas bases de datos solo puede ser utilizada por las entidades y empresas integrantes del grupo o conglomerado financiero.	exista una base de datos compartidas entre las entidades del conglomerado.	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.	entidad y empresa integrante del grupo o conglomerado financiero. Asimismo, las bases de datos ~~la plataforma tecnológica donde se procesen estas 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 ~~por las entidades y empresas integrantes del grupo o conglomerado financiero~~.
Las bases de datos, las aplicaciones, los sistemas de información y las soluciones tecnológicas deben estar declarados en el perfil tecnológico.	**[260]CAJAANDE Pregunta** ¿Estas deben ser declaradas en el perfil tecnológico dependiendo de la gestión de TI que se determine según el artículo 16 (individual o corporativa)?	**[260]No procede** Se atiende como consulta. Se remite según las disposiciones del artículo 42, que indica entre otras que: Las entidades y empresas supervisadas deben elaborar su perfil tecnológico y actualizarlo anualmente. En los casos en que se cuente con una gestión de TI corporativa, un Comité de TI corporativo o sus respectivas funciones equivalentes a nivel corporativo, el grupo o conglomerado financiero podrá remitir un único perfil tecnológico al supervisor responsable.	Las bases de datos, las aplicaciones, los sistemas de información y las soluciones tecnológicas deben estar declarados en el perfil tecnológico.
	[261]ABC Se recomienda limitar el alcance a los procesos críticos definidos e identificados por la entidad bancaria. Debe considerarse que mantener un acceso "sin restricciones ni condiciones" a las Superintendencias a todas las bases de datos, sistemas y aplicaciones del Banco compromete la seguridad de la información y la protección de datos personales de los clientes. Si bien se entiende el espíritu de la disposición, deben establecerse	**[261] Procede** Se ajusta la redacción. Además, se aclara que las superintendencias no solicitan permisos privilegiados o de escritura a las bases de datos, sistemas, aplicaciones o plataformas tecnológicas.	

	condiciones de acceso acorde con las funciones de supervisión, de manera que se satisfagan ambos objetivos: el de la supervisión y el de la protección de los datos. Por otro lado, debe especificarse si la frase "sin ningún tipo de restricción o condición" implica que pueden solicitar permisos privilegiados o de escritura. Adicionalmente, ni la norma ni los lineamientos son claros en cuanto a cómo se protegerán dichos accesos. Es preciso aclarar qué se debe entender en la norma por "separación de los registros de cada entidad" para el caso de que exista una base de datos compartida entre las entidades del conglomerado.		
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.	**[262]COOPEMEP** Se solicita la formulación de la "Sección III. Lineamientos relacionados con las pautas para la implementación de los controles para la adquisición o el desarrollo del ciclo de vida del software." Conociendo las diferencias de los sectores, esto debería ser gradual pues podría requerir de migraciones de los sistemas de información que no representan un riesgo"	**[262] No procede** Se agregó una disposición transitoria para abordar el tema de identificación de brechas y la implementación de las disposiciones del reglamento.	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.
	[263]FEDEAC Valorar reformular la Sección III de los Lineamientos Generales del Reglamento General de Gestión de la Tecnología de Información. Conociendo las diferencias de los	**[263] No procede** Se agregó una disposición transitoria para abordar el tema de identificación de brechas y la implementación de las disposiciones del reglamento.	

	sectores, esto debe ser gradual pues podría requerir de migraciones de los sistemas de información que no representan un riesgo.		
	[264]COOPEBANPO Solicitar la reformulación de la "Sección III. Lineamientos relacionados con las pautas para la implementación de los controles para la adquisición o el desarrollo del ciclo de vida del software." Conociendo las diferencias de los sectores, esto debería ser gradual pues podría requerir de migraciones de los sistemas de información que no representan un riesgo "Las pautas no consideran una gradualidad para su implementación, tampoco son claras respecto a los sistemas actuales que poseen las entidades y que no cumplen con los requisitos. Hacer un cambio de CORE o cambiar un sistema puede llegar a ser sumamente oneroso y podría tomar varios años realizarlo. De igual forma pedirle a un proveedor modificar un sistema para incluir lo que se establece en las pautas podría acarrearle costos altos a las entidades o rompimiento de contratos y búsqueda de nuevos proveedores.	**[264] No procede** Se agregó una disposición transitoria para abordar el tema de identificación de brechas y la implementación de las disposiciones del reglamento.	
	[265]AAP Se solicita ampliar el punto, donde se especifique que la aplicabilidad es para bases de datos de producción o desarrollo con presencia de datos sensibles.	**[265] No procede** Las disposiciones del artículo hacen referencia directa a los controles de las aplicaciones, sistemas de información y soluciones tecnológicas, para que estas sean seguras, y no específicamente a las	

	Fuentes de información que no contengan datos que comprometan la seguridad, no necesitaría tener los controles mencionados. Se solicita la reformulación de la "Sección III. Lineamientos relacionados con las pautas para la implementación de los controles para la adquisición o el desarrollo del ciclo de vida del software", para establecer que pasa con los desarrollos anteriores al cambio regulatorio y los que están en proceso. Conociendo las diferencias de los sectores, esto debería ser gradual pues podría requerir de migraciones de los sistemas de información, existen piezas de software que no se consideran críticas y que no representan un riesgo, y no deberían aplicársele toda la regulación.	bases de datos, las cuales podrían tener otros mecanismos distintos. Las entidades serán las que definan los controles para gestionar sus diferentes ambientes para el desarrollo del ciclo de vida de software, en función de sus riesgos. Adicionalmente, para la implementación de las brechas que pueda tener la entidad con relación a las disposiciones del presente reglamento se incluyó un transitorio.	
	[266]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, para quienes el cumplimiento de todas las medidas exigidas para el desarrollo de software sería sumamente costoso o imposible de cumplir. Al impedir a las entidades bancarias acceder a soluciones tecnológicas que no cumplan con todas las medidas, se podría estar fomentando la concentración de proveedores y la exclusión de	**[266] 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.	

	emprendimientos y PyMES tecnológicas, así como limitar el acceso a soluciones informáticas de interés para las entidades. Es preciso que la normativa establezca un balance que no excluya del mercado a estos proveedores.	En todo caso, la externalización de bienes y servicios no puede poner en riesgo la estabilidad de la entidad.	
	[267]CB 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, para quienes el cumplimiento de todas las medidas exigidas para el desarrollo de software sería sumamente costoso o imposible de cumplir. Al impedirle a las entidades bancarias acceder a soluciones tecnológicas que no cumplan con todas las medidas, se podría estar fomentando la concentración de proveedores y la exclusión de emprendimientos y PyMES tecnológicas. Se recomienda valorar alternativas para garantizarle acceso de mercado a estos proveedores.	**[267] 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.	
	[268]SEGUROSLAFISE Se solicita ampliar el punto, donde se especifique que la aplicabilidad es para bases de datos de producción o desarrollo con presencia de datos sensibles. Fuentes de información que no contengan datos que comprometan la seguridad, no necesitaría tener los controles mencionados. Se	**[268] No procede** 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. El aspecto esencial está dirigido a la debida diligencia que deben realizar las entidades en relación con proveedores.	

	solicita la reformulación de la "Sección III. Lineamientos relacionados con las pautas para la implementación de los controles para la adquisición o el desarrollo del ciclo de vida del software", para establecer que pasa con los desarrollos anteriores al cambio regulatorio y los que están en proceso. Conociendo las diferencias de los sectores, esto debería ser gradual pues podría requerir de migraciones de los sistemas de información, existen piezas de software que no se consideran críticas y que no representan un riesgo, y no deberían aplicársele toda la regulación.	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.	
	[269]COOPENAE (Impacto Alto, Esfuerzo Alto) El desarrollo de software profundiza en las prácticas de seguridad que deben ser aplicadas en el proceso y permite entender la necesidad de llevar metodologías modernas como "DevSecOps" y desarrollos ágiles.	**[269] No procede** Se mantiene la redacción propuesta.	
	[270]CIS Se sugiere la reformulación de la "Sección III. Lineamientos relacionados con las pautas para la implementación de los controles para la adquisición o el desarrollo del ciclo de vida del software." Conociendo las diferencias de los sectores, esto debería ser gradual pues podría requerir de migraciones de los sistemas de información que no representan un riesgo"	**[270] No procede** Se agregó una disposición transitoria para abordar el tema de identificación de brechas y la implementación de las disposiciones del reglamento.	

	[271]ISACA Este artículo debe ser integrado a los lineamientos de gestión de cambios, ya sea que se exijan procesos independientes para la gestión de cambios en los SI y para la gestión de cambios del resto de la infraestructura tecnológica. La gestión de cambios de SI es un foco de incidentes, roll back, y reprocesos, razones por las cuales se debería exigir un proceso de gestión de cambios exclusivo para el mantenimiento o adquisición de SI.	**[271] No procede** La propuesta de modificación reglamentaria no incluye lineamientos de gestión de cambios.	
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 el modelo de responsabilidades compartidas para proteger la infraestructura en la que se ejecutan los servicios que se ofrecen en la nube.	**[272]Luis Diego León Barquero** De acuerdo con las buenas prácticas, considero que se debe cambiar este párrafo: “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.” Se debe	**[272] Procede** Se ajusta la redacción considerando parte de lo sugerido.	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 ~~el modelo de responsabilidades compartidas~~ para proteger los datos, el software, la plataforma y la infraestructura en la ~~que se ejecutan los servicios que se ofrecen en la~~ nube.

	cambiar de acuerdo con las siguientes buenas prácticas: a. Las entidades no pueden delegar la responsabilidad, pueden utilizar servicios críticos con terceros, pero nunca delegar la responsabilidad. b. El modelo de responsabilidades compartidas es contrario a las buenas prácticas de administración, pues no existe el concepto de responsabilidades compartidas. Sugiero que este párrafo sea cambiado por el siguiente: Cuando las entidades y empresas supervisadas usen sus procesos críticos a través de servicios de computación en la nube, deben establecer claramente las responsabilidades compartidas de cada parte (usuario y proveedor de servicio) para proteger la infraestructura en la que se ejecutan los servicios que se ofrecen en la nube.		
	[273]MUCAP 1) No existe claridad sobre el alcance de este modelo. 2) Es muy complejo asegurar los apartados a, b y c, porque por lo general los proveedores son internacionales, cuyo marco legal está fuera de la regulación legal costarricense, y las empresas proveedoras no aceptan que se aplique la normativa y jurisdicción local, prevaleciendo la de los países de primer mundo conforme a los Principios de UNIDROIT y de la Convención de las Naciones Unidas de compraventa	**[273]Procede** Se ajusta la redacción y se elimina lo siguiente: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	

	internacional de mercancías (Convención de Viena) Adicionalmente, no existe claridad que sobre lo que se debe interpretar por certeza razonada.		
	[274]FEDEAC No queda claro cómo determinar el alcance de qué tipo de aplicativos deben cumplir con los estándares requeridos para este fin o si es requerido para cualquier aplicación o proveedor de servicios. ¿A qué se refieren con modelo de responsabilidades compartidas? ser más específicos. Para que el superintendente sea quien emita el criterio de riesgo sobre la infraestructura debe comprender la arquitectura, considerar si el supervisor quiere asumir esa responsabilidad. b) y c) No queda claro cuál es el acceso que el supervisor estaría necesitando y cuál es el patrón de razonabilidad de seguridad que se estaría buscando. Aplican los comentarios indicados en el artículo 20.	**[274] No procede** Se ajustó la redacción como parte de la observación sin hacer referencia a un modelo. Por otra parte, se eliminó lo siguiente: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	
	[275]VIDAPLENA En cuanto o cuando esto sea posible, dado que esto no aplicaría para contratos de Adhesión. ¿Seguridad en que porcentaje (los contratos adhesión no garantizan 100%) como se decidiría esto?	**[275] No procede** Se elimina el siguiente texto: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista	

		certeza razonada sobre la seguridad de la información y la cibernética".	
	[276]CFBNCR Se sugiere modificar el 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. Según lo que define el artículo 23 Obligaciones generales para el uso de la computación en la nube, el proveedor debe cumplir con una serie delineamientos muy específicos como lo es la certificación ISO 27001 y el cumplimiento de los estándares o buenas prácticas, tales como las ISO 27017 y27018. Por lo anterior, se recomienda sensibilizar las disposiciones de la norma con lo establecido a nivel de la legislación vigente, por ejemplo, los artículos17 y 34 de la Ley General de Contratación Pública; de manera que sea posible garantizar que existe oferta suficiente en el mercado local y/o regional, que permita suplir los diferentes tipos de servicios en la nube que las organizaciones requieren, cumpliendo con los requisitos que la norma establece,	**[276] No procede** Se ajustó la redacción como parte de la observación sin hacer referencia a un modelo y se eliminó el siguiente texto: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	

	a un costo razonable. En este contexto, se considera necesario que el regulador pueda realizar una revisión general con respecto al cumplimiento tanto de los proveedores actuales como potenciales ante estos nuevos lineamientos, considerando eventualmente la existencia de un mecanismo para acreditación de las diferentes certificaciones que pueda tener un proveedor, que puedan sustituir o complementar las antes mencionadas, tal como lo permite el artículo.		
	[277]ABC 1-Es importante aclarar que las normas comprendidas en la sección III aplican únicamente para la nube pública. 2-Por otro lado, no resulta claro cómo se debe interpretar el punto b, referido al acceso al supervisor. Específicamente, se ha planteado la duda de si esto quiere decir que no se pueden adquirir servicios en nube tercerizados si el supervisor no tiene acceso a las plataformas.	**[277] No procede** 1-Las disposiciones son para el control de los servicios externalizados a través de proveedores de computación en la nube, indistintamente del tipo de modelo de implementación de la nube (Publica, privada o hibrida). 2- Se ajustó la redacción como parte de la observación sin hacer referencia a un modelo y se eliminó el siguiente texto: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	
	[278]OPC-CCSS 1. Se debe aclarar el tipo de computación en la nube a la que se	**[278] No procede** 1-Las disposiciones son para el control de los servicios externalizados a través	

	hace alusión dado que existe el modelo de nube pública, privada o híbrida. 2. Se sugiere aclarar el punto b, donde se menciona que "no se brinde acceso al supervisor", dado que se interpreta que no se podrían adquirir servicios en nube tercerizados si el supervisor no posee acceso a la plataforma. 3. Respecto a la condición de certeza razonada indicada en el inciso c, es un término ambiguo y sujeto de interpretación lo cual va en contra de la objetividad que debe tener el regulador en este tipo de condiciones.	de proveedores de computación en la nube, indistintamente del tipo de modelo de implementación de la nube (Publica, privada o hibrida). 2- Se ajustó la redacción como parte de la observación sin hacer referencia a un modelo] y se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética”.	
	[279]CB Se sugiere modificar el 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.	**[279] No procede** Se ajustó la redacción como parte de la observación sin hacer referencia a un modelo	
	[280]COOPENAE (Impacto Alto, Esfuerzo Alto). Los servicios que se adquieran en la nube deben estás sujetos a certificaciones ISO27001 o SOC2.	**[280] 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	

	Por la naturaleza de atestiguamiento de las auditorías, esto podría ocasionar que el precio de los servicios de terceros se incremente por el esfuerzo que les significa un proceso certificado SOC2 o ISO27001.	modelo de negocio, cuando se externalizan bienes y servicios críticos de TI a través de proveedores de servicios en la nube. Por otra parte, la mayoría de los proveedores de servicios de computación en la nube publican en sus sitios web información sus programas de conformidad para ayudar a sus clientes a comprender los controles instaurados por cada proveedor, con el fin de mantener la seguridad y la conformidad de la nube.	
	[281]BCR • Inciso c). ¿Si la información que se mantiene en nube es clasificada como sensible o crítica para la continuidad de negocio, se debe descartar la opción de computación en la nube? • Inciso b) y c). ¿Quiere decir que, bajo un servicio en nube tercerizado, si no se le brinda acceso al Supervisor, no puede ser contratado? ¿Qué pasaría con proveedores de servicios que están migrando a nube y solo dan los servicios bajo ese modelo y alguna de estas condiciones no se cumpla? • ¿Qué pasaría con proveedores de servicios que están migrando a nube y solo dan los servicios bajo ese modelo y alguna de estas condiciones no se cumpla? • ¿Qué tanto se ha socializado este tipo de consideraciones con dichos proveedores o sus Partners por parte del ente regulador?; lo anterior con el propósito de asegurar razonablemente su	**[281] No procede** Se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética”.	

	implementación en la práctica y obtener lo requerido. • Se solicita ampliar cuando es un SAAS.		
	[282]ISACA 1-El cuestionamiento está en si ¿puede llegarse a dar el caso que una entidad o empresa supervisada no tenga nada on premise? Se deben dictar las pautas para determinar que sí y qué no se puede gestionar en la nube, o que tipo de nube es la permitida, sea híbrida o pública, y si en el caso de que los servicios críticos están en nube esta debe ser híbrida, es solo un ejemplo, se requieren definir los términos en % o en desempeño y capacidad. 2-Con el propósito de evitar que esto se entienda como una "conectividad directa" a los datos en la nube y que esto le traslade al supervisor u organismo auditor responsabilidades en cuanto a la aplicación y efectividad de controles que garanticen la seguridad o privacidad de los datos en dicha conectividad, se podría mejorar la redacción para indicar "...deben garantizar la disposición y el acceso a la información requerida por las Superintendencias para poder ejercer sus labores de supervisión, sin ningún tipo de restricción o condición requerida."	**[282] No procede** 1-Las entidades y empresas supervisadas pueden seleccionar el modelo de implementación y el modelo de servicios de conformidad con su tamaño, complejidad y modelo de negocio. 2-Se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética”.	
Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando:	**[283]COOPEMEP** Para que el superintendente sea quien emita el criterio de riesgo sobre la infraestructura debe	**[283] No procede** Se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la	~~Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando:~~

	comprender la arquitectura, considerar si el supervisor quiere asumir esa responsabilidad.	infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	
	[284]COOPEBANPO Para que el superintendente sea quien emita el criterio de riesgo sobre la infraestructura debe comprender la arquitectura, considerar si el supervisor quiere asumir esa responsabilidad y como lo haría, porque a como está planteado no es claro. ¿Quién determinará que los requisitos a) b) y c) no se cumplen?	**[284] No procede** Se eliminó el siguiente texto: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	
	[285]INS Se estima que se le están otorgando al Supervisor facultades que son propias de la administración de las entidades supervisadas, por cuanto en las tres normas, en ese respectivo orden, se faculta al supervisor para requerir: conformación de comité de TI individual, gestiones de TI individuales, así como infraestructuras de almacenamiento diferentes a las adoptadas por las supervisadas.	**[285] Procede** Se eliminó el siguiente texto: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	

	[286]CIS Para que el superintendente sea quien emita el criterio de riesgo sobre la infraestructura debe comprender la arquitectura, considerar si el supervisor quiere asumir esa responsabilidad	**[286] No procede** Se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética”.	
a) no se cumplan los requisitos legales y de seguridad;			~~a) no se cumplan los requisitos legales y de seguridad;~~
b) no se brinde acceso al supervisor, o	**[287]COOPEANDE** b) No se brinde acceso al supervisor, c) "..no exista certeza razonada..". ¿No queda claro cuál es el acceso que el supervisor estaría necesitando?, y cuál es el patrón de razonabilidad de seguridad que se estaría buscando?. Aplican los comentarios indicados en el artículo 20.	**[287] No procede** Se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética”.	~~b) no se brinde acceso al supervisor, o~~
c)la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética.	**[288]BPDC** En el punto b, no queda claro el alcance de este punto. ¿El supervisor mencionado sería de la superintendencia?	**[288] No procede** Se eliminó el siguiente texto: “Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad;	~~c)la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética.~~

		b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	
	[289]CATHAY No nos queda claro a que hace referencia el término: "Certeza Razonada". ¿Con que criterio determinamos esta certeza razonada?	**[289] No procede** Se eliminó el siguiente texto: "Las Superintendencias pueden requerir un modelo de gestión de la infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando: a) no se cumplan los requisitos legales y de seguridad; b) no se brinde acceso al supervisor, o c) la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética".	
Artículo 23. Obligaciones generales para el uso de la computación en la nube			**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:	**[290]BPDC** Este tema debería ser parte del documento de gobierno de nube, además, se debe solicitar el grado de cumplimiento al proveedor actual de nube. arde acuerdo con el diseño de la solución y los componentes implementados, agregar un nuevo respaldo incrementa los costos y la administración. En el punto b, se recomienda ajustar la redacción de los criterios para que no sea una lista limitada a solo estos y se puedan adicionar otros. En el punto f, hay q considera que, si el contrato con el proveedor de	**[290] Procede** Se modifica el inciso f con la siguiente redacción: 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. Por otra parte, las entidades y empresas supervisadas deben cumplir las disposiciones de la presente propuesta a través de los distintos controles administrativos dispuestos por estas,	Las entidades y empresas supervisadas que utilicen servicios de computación en la nube deben:

	nube asegura la protección y disponibilidad de la información debido a que el proveedor cuenta con múltiples sitios de operación que dan continuidad al servicio en los niveles aceptables, por qué hay que adicionalmente tener respaldos en otro lugar?	para atender sus riesgos, lo anterior, considerando su tamaño, complejidad y modelo de negocio. Se ajusta la redacción del inciso b.	
	[291]MUCAP 1) Existe la incertidumbre sobre el proceder con los contratos que, previo a esta normativa; ya están vigentes. 2) No queda claro si esto sería mandatorio para todos los proveedores de servicios en la nube o solo para los que se certifiquen con otros estándares diferentes al 27001. 3) El inciso c y de, representan un esfuerzo importante siendo un reto para las entidades debido a que se requiere mucha capacidad para gestionar ambas verificaciones, siendo relevante también para los proveedores en su cumplimiento. 4) No queda si puede ser otro sitio dentro de la misma nube, como ejemplo se puede citar otra zona de disponibilidad de "Azure". 5) Es importante que se amplié lo relacionado con el "control de la administración de usuarios y privilegios", ya que los accesos y privilegios a los servicios de los proveedores es muy propio de cada entidad.	**[291] No procede** 1-Se incluyó la disposición transitoria denominada "Contratos con proveedores de bienes y servicios de TI" 2-La disposición aplica para todos los proveedores de servicios de computación en la nube. 3-La mayoría de los proveedores de servicios de computación en la nube publican en sus sitios web información sus programas de conformidad para ayudar a sus clientes a comprender los controles instaurados por cada proveedor, con el fin de mantener la seguridad y la conformidad de la nube. 4-El texto ya fue modificado. 5-Las entidades y empresas supervisadas deben definir 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 servicio de computación en la nube, así como los controles administrativos y técnicos asociados a este tipo de servicios 6-Se incluyó una disposición transitoria relacionada con identificación de	

	6) Esto representa una inversión importante para las entidades por lo que toma valor que se analice los costos para las entidades a raíz de este requerimiento. 7) Al plantear este inciso de esta manera no queda claro cómo ejecutar la operativa que permita dar observancia a lo indicado en este inciso, ya que ante un tercero solo se podría dejar a nivel contractual la responsabilidad. Como ejemplo se puede citar el efecto en las multinacionales donde el poder de negociación es muy bajo (Microsoft), eliminado una funcionalidad que la entidad requiera. 8) No existe claridad hasta dónde llega la cadena de abastecimiento para efectos de estos controles. 9 No existe claridad sobre lo indicado "diferentes rutas", debido a que nivel de la nube esta indicación queda muy amplia.	brechas e implementación de las disposiciones reglamentarias. 7-La observación no indica a cuál inciso se refiere. 8-La observación no indica a cuál inciso se refiere. 9-Se ajustó la redacción.	
	[292]JUPEMA En caso que un proveedor actual (ya contratado) no cumpla con las exigencias, ¿Cómo se procede? Se considera debe haber un período de transición o un transitorio para dicho fin, ¿cuál sería el plazo? ¿Aplica para todos los proveedores o solo los proveedores críticos?	**[292] Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	
	[293]COOPEMEP Se solicita eliminar c) Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001 y cumpla	**[293] No procede** La mayoría de los proveedores de servicios de computación en la nube publican en sus sitios web información sus programas de conformidad para ayudar a sus clientes a comprender los	

	con estándares o buenas prácticas, tales como las ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (System and Organization Controls por sus siglas en inglés) SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares. d) Verificar que, para los servicios de computación en la nube de los modelos de infraestructura como servicio (IaaS por sus siglas en inglés) y de plataforma como servicio (PaaS por sus siglas en inglés), el proveedor ofrezca un nivel TIER III o superior. Para el modelo de software como un servicio (SaaS por sus siglas en inglés), el nivel debe ser, al menos, TIER II. Solicitar como mínimo la explicación en los incisos c y d sobre los requisitos para el uso de la computación en la nube, de cómo interpretar la obligación de" Verificar", siendo que los proveedores, así como sistemas y servicios actuales podrían no cumplir con dichos requisitos, ¿y que en ciertos casos no sería viable su cumplimiento?	controles instaurados por cada proveedor, con el fin de mantener la seguridad y la conformidad de la nube. Se eliminó lo referente a los SOC. En relación con el inciso d), se modificó la redacción y se eliminó lo referente a TIER.	
	[294]FEDEAC 1En caso de que un proveedor actual no cumpla con las exigencias, se considera que debe de haber un período de transición o un transitorio para dicho fin, ¿cuál sería el plazo? ¿Aplica para	**[294]No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias. 2- Se considera que la certificación ISO 27001 permite dar razonabilidad sobre la	

	todos los proveedores o solo los críticos? c): ¿Qué pasa con los contratos vigentes? 2-Se estaría obligando a los proveedores a que cuenten con certificaciones ISO. Por favor explicar los incisos c y d sobre los requisitos para el uso de la computación en la nube, de cómo interpretar la obligación de "Verificar", siendo que los proveedores, así como sistemas y servicios actuales podrían no cumplir con dichos requisitos, y que en ciertos casos no sería viable su cumplimiento. La superintendencia no debe promover pocos proveedores en el sector financiero o condiciones monopólicas. La exigencia de certificaciones debe apegarse al tamaño de la entidad, nivel de madurez digital, apetito de riesgo, y estrategia de negocio.	gestión de la seguridad de la información, por lo que, es un aspecto que las entidades deberán observar. La mayoría de los proveedores de servicios de computación en la nube publican en sus sitios web información sus programas de conformidad para ayudar a sus clientes a comprender los controles instaurados por cada proveedor, con el fin de mantener la seguridad y la conformidad de la nube.	
	[295]COOPEBANPO 1-Implementar cifrado sobre información en reposo podría ser una labor que conlleve mucho tiempo en implementar considerando todos los cambios que esto podría acarrear sobre los sistemas actuales, en este aspecto se solicita considerar la eliminación de la palabra "en reposo" en el inciso 2-g) Con respecto a los incisos c y d sobre los requisitos para el uso de la computación en la nube, cómo interpretar la obligación de "Verificar", siendo que los proveedores, así como sistemas y	**[295] No procede** 1-Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias. Además, se ajustó la redacción de la disposición. 2-La mayoría de los proveedores de servicios de computación en la nube publican en sus sitios web información sus programas de conformidad para ayudar a sus clientes a comprender los controles instaurados por cada proveedor, con el fin de mantener la seguridad y la conformidad de la nube.	

	servicios actuales podrían no cumplir con dichos requisitos, ¿y que en ciertos casos no sería viable su cumplimiento?		
	[296]BAC Pregunta 1-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. ¿Es posible confirmar esta afirmación? 2-¿El supervisado puede aplicar su propia valoración para los servicios de terceros? 3.En la entidad contamos con proveedores para los que se tiene un "contratos de adhesión" como por ejemplo Microsoft/Oracle/VMware. Entendemos que para estos casos no se requieren las certificaciones indicadas en este artículo. ¿Es posible confirmar esta afirmación? 4. Si la entidad cuenta con un proveedor, que a su vez tiene un proveedor con servicios de computación en la nube, ¿Quién debe de tener la certificación? ¿El proveedor directo de la entidad o los proveedores del tercero?	**[296]No procede** Se atiende como consulta. 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. 2-Tal como se indica en el artículo No. 27 “Identificación, evaluación y monitoreo de los riesgos de tercerización de bienes y servicios de TI críticos”, las entidades y empresas supervisadas deben identificar, evaluar y monitorear, de conformidad con las políticas establecidas, los riesgos de tercerización de bienes y servicios de TI críticos, así como revelar dichos riesgos en el perfil tecnológico. 3-La mayoría de los proveedores de servicios de computación en la nube publican en sus sitios web información sus programas de conformidad para ayudar a sus clientes a comprender los controles instaurados por cada proveedor, con el fin de mantener la seguridad y la conformidad de la nube. 4-La entidades y empresas supervisadas deben garantizar que sus proveedores y la cadena de proveedores cuenten con los controles requeridos y establecidos por la entidad de conformidad con los bienes y servicios externalizados y su apetito, tolerancia y capacidad de riesgos.	
	[297]CAJAANDE	**[297]No procede**	

	F. e inciso I. ¿Esto lo debería tener la entidad o bien, el proveedor de servicio?	La propuesta se modificó para mejorar el entendimiento, de conformidad con el siguiente texto: 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 aseguren o incluyan el respaldo. i) Contar con sistemas de registro, monitoreo y alarma de eventos de incidentes de seguridad de la información y seguridad cibernética.	
	[298]CFBNCR 1-En el artículo 23 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-El punto b) no considera aspectos de disponibilidad ni capacidad, por lo que se sugiere ajustar la redacción de la siguiente manera: b) Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube, considerando la seguridad, fiabilidad, garantía de disponibilidad del servicio, capacidad, escalabilidad, costo, soporte, experiencia, interoperabilidad y cumplimiento regulatorio.	**[298] 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. 2-Se ajustó la redacción como parte de la observación 290. 3-Las entidades y empresas supervisadas deben establecer los controles técnicos de conformidad con su tamaño, complejidad, modelo de negocio y riesgos.	

	3-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.		
	[299]ABC 1-Sobre lo dispuesto en el inciso d, debe señalarse que las certificaciones TIER II y III que se solicitan al proveedor de nube no son técnicamente adecuadas ni pertinentes. Lo anterior debido a que estas son aplicables a data centers, y no a los servicios de nube como tales. Las certificaciones ISO 27001, 27017, y los procesos SOC2, sí son aplicables y son suficientes para garantizar una adecuada seguridad de la información procesada y almacenada por el proveedor cloud. 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. 3-Sobre el inciso f, se plantea la consulta de si el control a que se refiere esta disposición puede ser transferido al proveedor del servicio en la nube mediante el uso de sus centros de datos. Es preciso aclarar si las certificaciones serían requeridas de acuerdo con la clasificación de datos que se vayan a compartir con el proveedor. ¿Cuál es el tratamiento de este requisito para los contratos de adhesión, como por ejemplo, con Microsoft u otros similares?	**[299] Procede** 1-Se modifica la redacción del incido c y d. 2-Respecto al punto 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. 3-Se modificó la redacción.	

	¿Pueden las entidades aplicar su propia valoración para los servicios de terceros?		
	[300]OPC-CCSS 1. Se debe aclarar el tipo de computación en la nube a la que se hace alusión dado que existe el modelo de nube pública, privada o híbrida. 2. No se aclara en el punto c cuáles estándares o mejores prácticas sustituyen o modifican la certificación ISO 27001 o la SSAE16/SSAE18 (punto d) lo cual se considera una ambigüedad que imposibilita garantizar la objetividad con la cual debe ser tratado un reglamento. 3. Se sugiere especificar de qué tipo deben ser los TIER (diseño, construcción, operación) ya que no se indica eso en el reglamento. 3. Dependiendo del modelo de servicio contratado, si un proveedor es el gestor de administración de usuarios y privilegios, por ejemplo, en una plataforma compartida, el inciso h del reglamento no podría ser cumplido y limita los servicios a los que pueden acceder los clientes basados en nube pública. 4. 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.	**[300] No procede** 1-Las disposiciones son para el control de los servicios externalizados a través de proveedores de computación en la nube, indistintamente del tipo de modelo de implementación de la nube (Publica, privada o hibrida). 2 y 3 -La redacción fue modificada. 4-Es responsabilidad de las entidades y empresas supervisadas velar que se establezcan los controles técnicos y administrativos para la gestión y de usuarios y sus privilegios, indistintamente del proveedor del servicio.	
	[301]CB	**[301]No procede** 1-Se modificó la redacción.	

	1-Inciso f: Comentarios: Sobre la obligación del inciso f), si el contrato con el proveedor de nube asegura la protección y disponibilidad de la información debido a que el proveedor cuenta con múltiples sitios de operación que aseguran la continuidad del servicio en los niveles aceptables, ¿por qué se solicita tener respaldos adicionales en otro lugar? Se solicita realizar la aclaración con criterios técnicos e incluirlo dentro del reglamento. Tampoco queda claro si puede ser otro sitio dentro de la misma nube, como ejemplo se puede citar otra zona de disponibilidad de "Azure". Asimismo, se solicita aclarar si el sitio alterno puede brindarlo el mismo proveedor del servicio en la nube, mediante el uso de sus centros de datos. 2-Inciso i: Comentarios: Esto representa una inversión importante para las entidades, por lo que es indispensable dar un plazo razonable para que las entidades puedan planificar y asumir los costos de este requerimiento. 3-Inciso j: Comentarios: Lo establecido en el inciso j) es lo ideal, pero su ejecución operativa es muy complicada por la privacidad, por lo que ante un tercero solo se podría avanzar a nivel contractual la responsabilidad. Como ejemplo se puede citar el efecto en las multinacionales, donde el poder de	2-Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias. 3-Es responsabilidad de las entidades y empresas supervisadas velar por que se establezcan los controles técnicos y administrativos para la gestión de los proveedores, acuerdos de niveles de servicio y de los riesgos de la externalización, indistintamente del proveedor del servicio. 4-Las entidades y empresas supervisadas deben establecer los controles técnicos de conformidad con su tamaño, complejidad, modelo de negocio y riesgos.	

	negociación es muy bajo (ejemplo Microsoft y otras), eliminado la posibilidad de personalizar el servicio. Inciso k: Comentarios: Aplica el mismo comentario y preocupación expuesta en el inciso j). No existe claridad hasta dónde llega la cadena de abastecimiento para efectos de estos controles. 4-Inciso l: Comentarios: 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. Adición que se sugiere al artículo 23: En el artículo 23 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".		
	[302]SEGUROSLAFISE Se sugiere eliminar el punto c y d de la obligatoriedad de esta norma. Los principales proveedores de servicios en la nube no cumplen con la totalidad de estos requisitos. Favor ampliar la aplicabilidad y en caso de ya utilizar servicios en la nube que no cumplan alguno de estos requisitos cómo se debe proceder (Ejemplo: Azure, AWS, Google, Oracle). ¿En qué casos no sería viables u cumplimiento? ¿Tier en qué fase? ¿En diseño? ¿En Operación? Si conservan este artículo, deben de ampliar. Existen contratos de servicios firmados en la actualidad que podrían tener	**[302] No procede** La redacción fue modificada.	

	penalizaciones por cambios o cancelaciones. Con esta regulación se estaría restringiendo el uso de herramientas de uso regular tales como Azure, AWS, Google que no cumplen con estas condiciones, Favor su aceptación en derogar la obligatoriedad Para el punto F: Favor aclarar que es referente solo a la información sensible/confidencial que se tenga en nube. Siendo la aseguradora la que decide qué información essensible /clasificada de acuerdo a las clasificaciones.		
	[303]COOPENAE Consideramos oportuno que, al ser temas de actualidad y consecuentemente cambiantes, que se permita implementar otro tipo de certificaciones, las cuales sean reconocidas a nivel internacional y que se equiparen a las certificaciones indicadas en la normativa en consulta. Incluso, que esto vaya alineado al apetito al riesgo de cada entidad, así como lo significativo que sean los negocios digitales en el modelo de negocio de cada una.	**[303] No procede** La redacción fue modificada. 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.	
	[304]CIS Se sugiere eliminar: c) Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001 y cumpla con estándares o buenas prácticas, tales como las ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que sustituyan o modifiquen las	**[304] No procede** La redacción fue modificada. Además, se eliminó lo referente a SOC y TIER. 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.	

	anteriores y debe disponer de informes de controles de organización de servicios (System and Organization Controls por sus siglas en inglés) SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares. d) Verificar que, para los servicios de computación en la nube de los modelos de infraestructura como servicio (IaaS por sus siglas en inglés) y de plataforma como servicio (PaaS por sus siglas en inglés), el proveedor ofrezca un nivel TIER III o superior. Para el modelo de software como un servicio (SaaS por sus siglas en inglés), el nivel debe ser, al menos, TIER II. Solicitar eliminar la información en reposo g) Mantener cifrada la información, cuyo uso o acceso esté clasificado como confidencial, ya sea en tránsito o en reposo, mediante el empleo de estándares y algoritmos reconocidos internacionalmente. Solicitar como mínimo la explicación en los incisos c y d sobre los requisitos para el uso de la computación en la nube, de cómo interpretar la obligación de "Verificar", siendo que los proveedores, así como sistemas y servicios actuales podrían no cumplir con dichos requisitos, ¿y que en ciertos casos no sería viable su cumplimiento?		
	[305]ISTMO 1-Inciso f) Mejorar esta redacción, a como está no hace distinción de que tipo de información, por lo	**[305] No procede** 1-La redacción fue modificada. 2-La redacción fue modificada.	

	cual se entendería que toda la información (100%). Esto debería de quedar sujeto a la información crítica que la organización defina, ejemplo: Bases de Datos de misión crítica, información financiera, etc. tener un sitio alterno se justifica totalmente basado en un análisis técnico como un BIA, pero esto no se aplica al 100% de la información de una organización. 2-Inciso l) Modificar la redacción, así como está estaría bien para un proveedor local que brinda tanto los servicios de nube como las comunicaciones, y está bien que se evalúe el uso de 2 rutas en los enlaces de comunicación; pero que pasa en los casos de nube pública, como Microsoft, Aws, OCI, Digital Ocean, etc? el proveedor de servicios de nube no brinda los servicios de comunicación, ésos los brinda un ISP Local. Así como esta redactado es confuso interpretar esto?		
	[306]CCPA El Colegio de Contadores Públicos de Costa Rica, recomienda que a estos requerimientos se le agregue la solicitud de un informe de aseguramiento basado de acuerdo con la Norma Internacional de Encargos de Aseguramiento (NIEA) 3402, Informe de Aseguramiento sobre los controles en las organizaciones de servicios, cuando se use un centro de servicios de esta naturaleza a fin	**[306]No procede** Las auditorías externas de TI se deben realizar conforme a lo establecido por el ITAF de ISACA, tal como se indica en el artículo 46 “Auditoría Externa de TI”	

	de corroborar el cumplimiento normativo.		
	[307]ISACA 1-En la obligación: "b) Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube", En algunos aspectos que podrían darse controversia en la manera en que se firma un contrato de adhesión con un proveedor de nube; ya que, una vez contratado el servicio, podría ser oneroso cambiar o adendar nuevas obligaciones en la relación comercial. Este es uno de los aspectos donde el ente fiscalizador debe dictar las pautas, no dejarlo discrecional. 2-Los ítems 23.c en adelante son algunos de los criterios para seleccionar el proveedor de nube, precisamente estos responden al ítem 23.b. 3-El apartado tiene un título confuso, existen criterios de selección de proveedor de nube y controles de implementación de dicho servicio, pero el título no es claro al respecto. 4-Con el propósito de evitar que esto se entienda como una "conectividad directa" a los datos de una base de datos y que esto le traslade al supervisor u organismo auditor responsabilidades en cuanto a la aplicación y efectividad de controles que garanticen la seguridad o privacidad de los datos en dicha conectividad, se podría mejorar la	**[307]No procede** 1-La redacción fue modificada. 2- La redacción fue modificada. 3-La disposición indica: “Obligaciones generales para el uso de computación en la nube” 4- La redacción fue modificada. 5-Se ajustó la redacción. 6-Se ajustó la redacción considerando parte de lo sugerido	

	redacción para indicar "...deben garantizar la disposición y el acceso a la información requerida por las Superintendencias para poder ejercer sus labores de supervisión, sin ningún tipo de restricción o condición requerida." 5-G Le agregaría al final la frase "como seguros de acuerdo con los estándares internacionales, las mejoras a debilidades identificadas o niveles de obsolescencia según la industria." 6-I Es importante especificar con lo que se requiere cumplir, debido que se deben diferenciar los "eventos" de los "incidentes" de acuerdo con las mejores prácticas de la industria. Los eventos son situaciones ocurridas u observables que no afectan la operación y los "incidentes" sí afectan la operación del negocio. No sé si acá lo importante es la "redundancia" más que las "diferentes rutas"		
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, considerando la seguridad, fiabilidad, escalabilidad, costo, soporte, experiencia, interoperabilidad y cumplimiento regulatorio.		Se modifica con la observación [290 b]	b) Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube~~, considerando~~. 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 y cumpla con estándares o buenas prácticas, tales como las ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que sustituyan o modifiquen las anteriores y debe disponer de	**[308]Luis Diego León Barquero** En el punto c, yo agregaría los aseguramientos basados en la Norma Internacional de Encargos de Aseguramiento 3402 Informes de aseguramiento sobre los controles en las organizaciones de	**[308] No procede** La redacción fue modificada. Además, se eliminó lo referente a SOC.	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 ~~y~~ cumpla con estándares o buenas prácticas, tales como las ISO 27017, ~~y~~ 27018 o las mejores prácticas del Cloud Security Alliance. ~~El~~

informes de controles de organización de servicios (System and Organization Controls por sus siglas en inglés) SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares.	servicios. En el punto c, "Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001 y cumpla con estándares o buenas prácticas, tales como las ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (System and Organization Controls por sus siglas en inglés) SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares." Yo sé que la mayoría de los entes que ofrecen servicios en la nube, por ejemplo, Azure y AWS, cuentan con informes de aseguramientos hechos por terceros. Pero no se indica que pasa si el proveedor de servicio de la nube no tiene ninguna certificación.		~~proveedor puede certificarse con estándares o mejores prácticas que sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (System and Organization Controls por sus siglas en inglés) SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares.~~
	[309]AAP 1-Se sugiere eliminar el punto c y d de la obligatoriedad de esta norma. Los principales proveedores de servicios en la nube no cumplen con la totalidad de estos requisitos. Favor ampliar la aplicabilidad y en caso de ya utilizar servicios en la nube que no cumplan alguno de estos requisitos cómo se debe proceder (Ejemplo: Azure, AWS, Google, Oracle). ¿En qué casos no sería viable su cumplimiento? ¿Tier en qué fase? ¿En diseño? ¿En Operación? Si conservan este artículo, deben de	**[309] No Procede** 1-La redacción fue modificada. Se eliminó lo referente a SOC y TIER. 2-La entidad es la responsable en establecer el alcance de los mecanismos de control, de conformidad con el tamaño, complejidad, modelo de negocio y los riesgos, adicionalmente, se modifica la redacción del inciso f. y se aclara que la disposición hace referencia a toda la información que se procesa y almacena en la nube	

	ampliar. Existen contratos de servicios firmados en la actualidad que podrían tener penalizaciones por cambios o cancelaciones. Con esta regulación se estaría restringiendo el uso de herramientas de uso regular tales como Azure, AWS, Google que no cumplen con estas condiciones, Favor su aceptación en derogar la obligatoriedad. 2-Con respecto al inciso f): Favor aclarar que es referente solo a la información sensible/confidencial que se tenga en nube. Siendo la aseguradora la que decide qué información es sensible/clasificada de acuerdo a las clasificaciones. Por otra parte: La clasificación de TIERs del Uptime Institute lo que busca es medir la disponibilidad y el rendimiento general de un centro de datos. Sin embargo, esta métrica no da la visión completa para nuevas tecnologías y modelos como la nube. En nube existen diferentes estrategias que se pueden implementar para obtener una alta disponibilidad y resiliencia, por ejemplo, la utilización de varios sitios. Los proveedores de nube ofrecen SLAs y reportes SOC 2 que permiten obtener certeza razonable de los controles que implementan en su infraestructura relacionados con (i) la seguridad física del centro de datos, (ii) la disponibilidad, (iii) los planes de contingencia y (iv) el plan de		

	respuesta ante incidentes. Adicionalmente, este sistema de clasificación limita a los proveedores de nube mantener la flexibilidad necesaria para ampliar y mejorar el rendimiento de la infraestructura de nube. Los proveedores de nube se centran en métricas que van más allá de lo que registran los niveles de Uptime Institute, como la automatización, la facilidad de escalado y la respuesta a los incidentes. Por lo anterior, es esencial que se permita la utilización de otros estándares o mejores prácticas, como el SOC2, para dar cumplimiento a este inciso. También es importante mencionar que el Uptime Institute no ha autorizado a otras organizaciones a certificar los centros de datos según su sistema de clasificación por niveles y no diseña, construye, ni opera centros de datos.		
d)Verificar que, para los servicios de computación en la nube de los modelos de infraestructura como servicio (IaaS por sus siglas en inglés) y de plataforma como servicio (PaaS por sus siglas en inglés), el proveedor ofrezca un nivel TIER III o superior. Para el modelo de software como un servicio (SaaS por sus siglas en inglés), el nivel debe ser, al menos, TIER II.	**[310]BCR** Inciso d). Qué pasa si el proveedor no puede ofrecer los requisitos indicados en dicho artículo, pero dentro del apetito de riesgo de la organización el que no lo tenga está dentro de la tolerancia definida, entonces, ¿no podemos contratar el servicio?, como por ejemplo: Verificar que, para los servicios de computación en la nube de los modelos de infraestructura como servicio (IaaS por sus siglas en inglés) y de plataforma como servicio (PaaS	**[310] Procede** Se modifica la redacción y se elimina lo referente a TIER. Se dejó la redacción de la siguiente forma: 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)Verificar que, para los servicios de computación en la nube de los modelos de infraestructura como servicio (IaaS por sus siglas en inglés) y de plataforma como servicio (PaaS por sus siglas en inglés), el proveedor ofrezca un nivel TIER III o superior. Para el modelo de software como un servicio (SaaS por sus siglas en inglés), el nivel debe ser, al menos, TIER II.~~ 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.

	por sus siglas en inglés), el proveedor ofrezca un nivel TIER III o superior. Para el modelo de software como n servicio (SaaS por sus siglas en inglés), el nivel debe ser, al menos, TIER II. o Para este listado de requerimientos, ¿se pueden gestionar excepciones o elementos deseables o todos son obligatorios, esto encarece los servicios y en otro escenario que pasa sino lo tiene y no lo necesitamos? ¿Qué pasa con los proveedores que no cuentan con certificaciones de seguridad de la información o con debilidades en acuerdos se servicio? o Valorar las excepciones, dado que actualmente las entidades tienen contratos con empresas como Microsoft y AWS, que no cuentan con un nivel TIER III o superior, y los servicios contratos son requeridos para el logro de los objetivos de la entidad. o Inciso f). en cuanto al sitio alterno, ¿es posible con el mismo proveedor de nube, pero en otra región o zona de disponibilidad? o Inciso j). Se solicita definir operaciones o cambios no deseados.		
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 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.		Se modifica con la observación [290 parte 2]	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, ya sea en tránsito o en reposo, mediante el empleo de estándares y algoritmos reconocidos internacionalmente.	**[311]SMSEGUROS** Considerar eliminar la palabra reposo del punto g. En caso que no se elimine, ampliar el término y a qué aplica.	**[311] 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.	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 ~~internacionalmente~~.
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.			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 de incidentes de seguridad de la información y seguridad cibernética.			i)Contar con sistemas de registro, monitoreo y alarma de eventos de incidentes de seguridad de la información y seguridad cibernética.
j) Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente.			j) Monitorear los servicios contratados para detectar operaciones o cambios no deseados y tomar acciones preventivas o correctivas oportunamente.
k) Monitorear el cumplimiento de los acuerdos de niveles de servicio establecidos con el proveedor de servicios en la nube y, en caso de que aplique, de sus subcontratistas.			k) Monitorear el cumplimiento de los acuerdos de niveles de servicio establecidos con el proveedor de servicios en la nube y, en caso de que aplique, de sus subcontratistas.
l)Contar con canales de comunicación con el proveedor de servicios en la nube, cifrados de extremo a extremo, y que, en lo posible, utilicen diferentes rutas.		Se modifica con la observación [291 - 9]	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 ~~diferentes rutas~~ 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**
Las entidades y empresas supervisadas deben mantener actualizada y a disposición de las Superintendencias la documentación de los servicios de computación en la nube relacionada con:	**[312]BPDC** Esto debería ser parte del documento de gobierno de nube, además, se debe solicitar el grado de cumplimiento al proveedor actual de nube. Existen servicios que por su naturaleza el respaldo	**[312] No procede** Se eliminó la parte de la disposición indicada en la observación. Además, se modificó el resto de la redacción del artículo para simplificar y mejorar el entendimiento.	~~Las entidades y empresas supervisadas deben~~ 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.

	está garantizado de acuerdo con el diseño de la solución y los componentes implementados, agregar un nuevo respaldo incrementa los costos y la administración. Sobre el punto a, se debe considerar que los procesos y procedimientos en la nube pueden corresponder al proveedor y no necesariamente el proveedor pone esa información a disposición en forma detallada pues es su sistema de entrega de servicios de nube que se puede considerar un factor competitivo diferencial. En otras palabras la organización supervisada podría no contar con acceso a ese nivel de documentación propia del proveedor. En el punto c, no es claro si se refiere a la topología de red de la organización supervisada para conectarse a Internet? Porque la topología de red interna del proveedor de servicios en la nube no está disponible. Los proveedores no van a presentar esa información primero porque constituye un diseño propio que genera ventajas competitivas, segundo, sería un riesgo de seguridad compartir esa información con sus clientes.		~~los servicios de computación en la nube relacionada con:~~
	[313]MUCAP 1) No queda en claro a qué tipos de informes de auditoría se refieren si son auditorías que hace el proveedor, o auditoría que las entidades le solicitan al proveedor,	**[313] No procede** Se eliminó la parte de la disposición indicada en la observación.	

	o por el contrario informes de la Auditoría Interna de cada entidad. Adicionalmente se solicita aclarar, en cuanto a que indica que debe "actualizarse anualmente"; podría crear confusión ya que los informes de auditoría externa tienen una periodicidad de dos años conforme artículo 48 2) Surge la misma inquietud del inciso anterior si este tipo de informes de riesgos serían análisis hechos por el proveedor, o por su parte análisis realizados por área de Gestión de Riesgos de cada entidad. 3) Con respecto al inciso g y h no existe claridad sobre el alcance de esta documentación.		
	[314]COOPESERVIDORES e) Aclarar el alcance esperado de la auditoria indicada en este inciso. h) Aclarar a que corresponde el Modelo esperado: si es una certificación, alcance de la auditoria mencionada en el inciso e.) (de ser así, ¿cuál?) u otro.	**[314] No procede** Se eliminó la parte de la disposición indicada en la observación.	
	[315]VIDAPLENA ¿El punto a) lo que se solicita es la información asociada a los procesos, servicios, procedimientos y aplicaciones de la empresa supervisada? c) Diagramas de red que permitan identificar la plataforma que soporta el servicio de computación en la nube contratado. Observación/ Consulta: ¿Hace referencia este punto al suministro de los diagramas de red internas de la empresa supervisada, donde se	**[315] No procede** Se eliminó la parte de la disposición indicada en la observación.	

	evidencie como parte de la topografía la inclusión de la nube?		
	[316]CFBNCR En este artículo se destaca la necesidad de fortalecer el monitoreo de los flujos aplicativos, lo cual es una necesidad creciente a nivel mundial. De acuerdo con una investigación publicada por la empresa Gartner en 2023, "solo el 47% de las organizaciones ha mapeado las dependencias de TI para sus actividades y aplicaciones críticas al menos de manera administrada", esto por cuanto los flujos aplicativos y los escenarios de pruebas (QA testing) "no logran desarrollarse a la misma velocidad que está cambiando el entorno productivo, debido a la evolución acelerada de los nuevos servicios y la necesidad de integraciones cada vez más complejas". En este sentido, se debe considerar que esta labor eventualmente va a requerir mucho tiempo e inversión por parte de las organizaciones supervisadas, tanto a nivel de personas, procesos y tecnologías para el monitoreo del rendimiento de aplicaciones (APM), de la experiencia digital (DEM) e inteligencia artificial (IA) para ITOps (AIOps); para lo cual se recomienda considerar una adopción incremental en el tiempo que se especifique en el reglamento.	**[316] No procede** Se eliminó la parte de la disposición indicada en la observación.	

	[317]ABC En la norma se destaca la necesidad de fortalecer el monitoreo de los flujos aplicativos. En este sentido, se debe considerar que esta labor va a requerir mucho tiempo e inversión por parte de las organizaciones supervisadas, tanto a nivel de personas, procesos y tecnologías para el monitoreo del rendimiento de aplicaciones, de la experiencia digital e inteligencia artificial para ITOps. Por esto se solicita una mayor transitoriedad. Por otro lado, no resulta claro cuál es la expectativa del regulador con el requerimiento de flujo de datos.	**[317] No procede** Se eliminó la parte de la disposición indicada en la observación.	
	[318]OPC-CCSS En el reglamento ni en los lineamientos se indica cómo operativizar este artículo y por ende, limita el claro entendimiento por parte del supervisado para su atención.	**[318] No procede** Se eliminó la parte de la disposición indicada en la observación.	
	[319]CB Inciso a: Comentarios Sobre la documentación solicitada en el punto a), debe tenerse en consideración que los procesos y procedimientos en la nube pueden corresponder al proveedor de manera directa y no necesariamente el proveedor pone esa información a disposición en forma detallada. En otras palabras, la organización supervisada podría no contar con acceso a ese nivel de documentación propia del proveedor. Inciso c: Comentarios	**[319] No procede** Se eliminó la parte de la disposición indicada en la observación.	

	Sobre este inciso, se solicita aclarar si el diagrama se refiere a la topología de red de la organización supervisada para conectarse a Internet. Lo anterior debido a que la topología de red interna del proveedor de servicios en la nube no está disponible. Los proveedores no presentan esta información por varias razones: primero, porque constituye un diseño propio que genera ventajas competitivas y segundo, debido a que sería un riesgo de seguridad compartir dicha información con los clientes. Inciso e: Comentarios Sobre los informes de auditoría, podría contener información de carácter confidencial del proveedor que no podría ser compartida con la entidad supervisada ni con la Superintendencia. No obstante, si el proveedor cuenta con certificaciones internacionales como las mencionadas (ISO27001, SSAE16/SSAE18 o similares), significa que ha sido auditado y que satisface los requerimientos establecidos en el estándar. Esa evidencia debería ser suficiente tanto para la entidad supervisada como para la Superintendencia. En tal sentido, es importante incluir esta alternativa en la redacción de este inciso.		
	[320]BCR • Inciso c). ¿Esto lo daría un proveedor que brinde un servicio	**[320] No procede** Se eliminó la disposición.	

	SSAS? ¿Hasta qué nivel de detalle se requiere? • Inciso e) ¿Estas Auditorías son evaluaciones que deben de contratar los proveedores? • Inciso f). Definir el alcance del término "variaciones" los cambios en los servicios en nube son muy normales. • ¿Si los proveedores no están de acuerdo o no las tienen debemos de prescindir de los servicios? • ¿Son todos estos elementos obligatorios o se pueden tener excepciones?		
	[321]CCPA Nuestra recomendación es realizar una aclaración en el punto C, con respecto a que tipo de Informes de auditoría se requieren, ya que pueden ser los realizados por la auditoría interna/ externa/ambas**.**	**[321] No procede** Se eliminó la disposición.	
a) Los procesos, los servicios, los procedimientos y las aplicaciones que se ejecutan en la nube.			~~a) Los procesos, los servicios, los procedimientos y las aplicaciones que se ejecutan en la nube.~~
b) Los flujos de datos de los procesos críticos del negocio que utilizan los servicios de computación en la nube.			~~b) Los flujos de datos de los procesos críticos del negocio que utilizan los servicios de computación en la nube.~~
c)Diagramas de red que permitan identificar la plataforma que soporta el servicio de computación en la nube contratado.	**[322]FEDEAC** c) Por seguridad esto deberá validarse, ¿cómo la superintendencia resguardará la información? Se debe considerar el tipo de información que brinda el fabricante.	**[322] No procede** Se eliminó la parte de la disposición indicada en la observación.	~~c)Diagramas de red que permitan identificar la plataforma que soporta el servicio de computación en la nube contratado.~~
d)Procedimientos para verificar el cumplimiento de los acuerdos y de los niveles de servicio establecidos con el proveedor.			~~d)Procedimientos para verificar el cumplimiento de los acuerdos y de los niveles de servicio establecidos con el proveedor.~~
e) Informes de auditoría, pruebas de seguridad en la nube y estado actual de los servicios contratados, los cuales deben actualizarse anualmente.	**[323]Luis Diego León Barquero** El punto c indica “Informes de auditoría, pruebas de seguridad en la nube y estado actual de los	**[323] No procede** Se eliminó la parte de la disposición indicada en la observación.	~~e) Informes de auditoría, pruebas de seguridad en la nube y estado actual de los servicios contratados, los cuales deben actualizarse anualmente.~~

	servicios contratados, los cuales deben actualizarse anualmente." Sin embargo, no se especifica que tipo de auditoría: externa, interna o ambas. Sería conveniente ampliar la explicación.		
	[324]COOPEBANPO ¿En el inciso e) se debe realizar una auditoría a los servicios de nube anualmente? A como está redactado implica que los informes de auditoría, las pruebas de seguridad y el estado actual de los servicios deben ser actualizados anualmente. Para las nubes públicas como a AWS y AZURE no es tan factible establecer acuerdos entre las partes, ya que muchos son contratos de adhesión, estos requerimientos dejarían por fuera el uso de nubes de este tipo. Por su parte los lineamientos hablan de cláusulas que se deben incorporar a los contratos, pero que en el caso de las nubes publicas esto no es factible realizarlo.	**[324] No procede** Se eliminó la parte de la disposición indicada en la observación.	
	[325]AAP Con respecto al inciso e): Favor aclarar, si la solicitud es contar con una auditoría de nube anual, y si es suficiente auditar la tenencia de una certificación o cuál es el alcance. Este punto se considera una excesividad en el control, parecen controles sobre controles, sabiendo que puntos anteriores ya están exigiendo certificaciones de servicios de nube y en efecto una certificación es para el aseguramiento de controles.	**[325] No procede** Se eliminó la parte de la disposición indicada en la observación.	

	[326]SEGUROSLAFISE Para el punto e: Favor aclarar, si la solicitud es contar con una auditoría de nube anual, y si es suficiente auditar la tenencia de una certificación o cuál es el alcance. Este punto se considera una excesividad en el control, parecen controles sobre controles, sabiendo que puntos anteriores ya están exigiendo certificaciones de servicios de nube y en efecto una certificación es para el aseguramiento de controles.	**[326] No procede** Se eliminó la parte de la disposición indicada en la observación.	
	[327]ISTMO Inciso e) No queda claro quién debe proveer esos informes de auditoría y pruebas de seguridad. Si fuese el proveedor de nube, ninguno los va a proveer, pues va en contra de la propia seguridad. Y en caso de tratarse de que las empresas reguladas las realicen, entonces qué sentido tiene que en el artículo 23ya regule que los proveedores de nube deben contar con certificaciones ISO 27,001 al obtener ésta son firmas certificadores que avalan estos puntos. Reconsiderar este inciso o reformularlo.	**327] No procede** Se eliminó la parte de la disposición indicada en la observación.	
f) Informes de riesgos actualizados, al menos, anualmente o cuando se presenten variaciones en los servicios.	**[328]CAJAANDE** F: Agradecemos ampliar si a lo que se refieren es un informe de riesgo actualizado con la información sobre los servicios que son soportados en la nube o bien del servicio de la nube en general.	**[328] No procede** Se eliminó la parte de la disposición indicada en la observación.	~~f) Informes de riesgos actualizados, al menos, anualmente o cuando se presenten variaciones en los servicios.~~
g) Informes anuales de monitoreo de servicios.			~~g) Informes anuales de monitoreo de servicios.~~

h) Modelo de seguridad establecido para el servicio de computación en la nube.			~~h) Modelo de seguridad establecido para el servicio de computación en la nube.~~
i)Contratos y acuerdos de niveles de servicios establecidos con el proveedor de los servicios de computación en la nube.			~~i)Contratos y acuerdos de niveles de servicios establecidos con el proveedor de los servicios de computación en la nube.~~
Sección IV. Tercerización de bienes y servicios de TI			**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.	**[329]MUCAP** 1) Se sugiere revisar el alcance de esta sección IV, ya que no queda claro si es para bienes y servicios "críticos" de TI que estén tercerizados, o para todos los bienes y servicios de TI tercerizados. 2) Se sugiere analizar el impacto operativo que le generaría para las entidades (capacidad). 3) No está claro el alcance de este párrafo hasta dónde debe llegar la cadena de suministro.	**[329]No procede** 1-La redacción de la disposición indica que se refiere a la tercerización de la información y de los bienes y servicios de TI 2-Si bien la entidad y empresa supervisada delega sus bienes y servicios de TI a terceros, la responsabilidad sigue siendo de la entidad y en caso de materializarse riesgos en el tercero, la entidad es la que debe responder ante sus partes interesadas. 3-Las entidades y empresas supervisadas en función de los bienes y servicios externalizados son las que deben evaluar los riesgos, considerando su apetito, tolerancia y capacidad de riesgos.	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.
	[330]COOPEMEP Texto sugerido: Se deben establecer controles a fin de comprobar que los proveedores que tercerizan bienes y servicios de TI implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los	**[330] No procede** Si bien la entidad y empresa supervisada delega sus bienes y servicios de TI a terceros, la responsabilidad sigue siendo de la entidad y en caso de materializarse riesgos en el tercero, la entidad es la que debe responder ante sus partes interesadas, por lo que la redacción de la propuesta mantiene la expectativa de alto nivel de las superintendencias para la gestión de los riesgos relacionados. Por su parte, el parrado indica que para	

	requerimientos de la entidades y empresas supervisadas.	dicha disposición se entiende por tercero a: proveedores, alianzas estratégicas, negocios conjuntos, convenios u otro tipo de arreglo comercial. Por otra parte, se modificó parte de la redacción de la disposición para mejorar el entendimiento.	
	[331]FEDEAC ¿Tercerización y tercero son términos que se deben manejar por aparte? ¿Cómo los está definiendo la Superintendencia? Párrafo tercero: Se sugiere el siguiente texto sustitutivo: Se deben establecer controles a fin de comprobar que los proveedores que tercerizan bienes y servicios de TI implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los requerimientos de la entidades y empresas supervisadas.	**[331] No procede** Si bien la entidad y empresa supervisada delega sus bienes y servicios de TI a terceros, la responsabilidad sigue siendo de la entidad y en caso de materializarse riesgos en el tercero, la entidad es la que debe responder ante sus partes interesadas, por lo que la redacción de la propuesta mantiene la expectativa de alto nivel de las superintendencias para la gestión de los riesgos relacionados. Por su parte, el parrado indica que para dicha disposición se entiende por tercero a: proveedores, alianzas estratégicas, negocios conjuntos, convenios u otro tipo de arreglo comercial. Por otra parte, se modificó parte de la redacción de la disposición para mejorar el entendimiento.	
	[332]CATHAY Interpretamos que con solo ser responsables y tener un método de supervisar el gobierno y la gestión de la seguridad de la información y seguridad cibernética, se pueden compartir datos con terceros, a través de la contratación de servicios de TI o alianzas estratégicas con terceros. ¿Es correcto?	**[332] No procede** Las entidades y empresas supervisadas son las responsables de establecer los controles para la entrega de sus bienes o servicios. Cuando estos son externalizados, se debe contar con los controles aplicables a fin de mantener un sistema de control interno que atienda los riesgos relacionados a estos.	
	[333]COOPEBANPO Texto sugerido: Se deben establecer controles a fin de comprobar que los proveedores	**[333] No procede** Si bien la entidad y empresa supervisada delega sus bienes y servicios de TI a terceros, la responsabilidad sigue siendo	

	que tercerizan bienes y servicios de TI para la entidad implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los requerimientos de la entidades y empresas supervisadas.	de la entidad y en caso de materializarse riesgos en el tercero, la entidad es la que debe responder ante sus partes interesadas, por lo que la redacción de la propuesta mantiene la expectativa de alto nivel de las superintendencias para la gestión de los riesgos relacionados. Por su parte, el parrado indica que para dicha disposición se entiende por tercero a: proveedores, alianzas estratégicas, negocios conjuntos, convenios u otro tipo de arreglo comercial. Por otra parte, se modificó parte de la redacción de la disposición para mejorar el entendimiento.	
	[334]CAJAANDE ¿Esto aplicaría en caso de que la gestión de TI sea declarada como corporativa según el artículo 16?	**[334]No procede** No queda claro a que se hace referencia en l consulta cuando indican “Esto”.	
	[335]OPC-CCSS Se sugiere aclarar de qué forma se aplicaría la resiliencia operativa digital para la adquisición de bienes.	**[335] 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. Las entidades y empresas supervisadas definen el cómo aplicar esta disposición de conformidad con su modelo de negocio, tamaño, complejidad y riesgos.	
	[336]CB Sobre este artículo y la Sección IV de los Lineamientos Generales, se recomienda al regulador evaluar la necesidad, idoneidad y proporcionalidad de cada uno de los elementos y subelementos indicados en la sección IV de los Lineamientos y disminuir el listado de elementos obligatorios, dejando un margen de discreción a las partes para que determinen libremente en sus contratos, cómo	**[336] No procede** Los lineamientos generales de la propuesta de modificación reglamentaria indican entre otras, que las entidades y empresas supervisadas establecerán los elementos que se incorporarán en el diseño de los contratos y los acuerdos de nivel de servicio de TI que celebren con sus proveedores, de conformidad con los riesgos del bien o servicio de TI tercerizado.	

	cumplir con los objetivos de interés público perseguidos. Podría haber secretos comerciales involucrados y otros datos relevantes y sensibles para las organizaciones (como el precio), que se revelarían al regulador sin realmente ser necesario para el fin público perseguido.	El interés del supervisor es conocer la gestión de los riesgos relacionados con los contratos y acuerdos de niveles de servicio, más que conocer secretos comerciales.	
	[337]SMSEGUROS Tercero y tercerización son conceptos diferentes. Por favor considerar replantear la redacción del párrafo de la siguiente manera: "Se deben establecer controles a fin de comprobar que los proveedores que tercerizan bienes y servicios de TI implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los requerimientos de la entidades y empresas supervisadas."	**[337] No procede** Si bien la entidad y empresa supervisada delega sus bienes y servicios de TI a terceros, la responsabilidad sigue siendo de la entidad y en caso de materializarse riesgos en el tercero, la entidad es la que debe responder ante sus partes interesadas, por lo que la redacción de la propuesta mantiene la expectativa de alto nivel de las superintendencias para la gestión de los riesgos relacionados. Por su parte, el parrado indica que para dicha disposición se entiende por tercero a: proveedores, alianzas estratégicas, negocios conjuntos, convenios u otro tipo de arreglo comercial. Por otra parte, se modificó parte de la redacción de la disposición para mejorar el entendimiento.	
	[338]CIS Texto sugerido: Se deben establecer controles a fin de comprobar que los proveedores que tercerizan bienes y servicios de TI implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los	**[338] No procede** Si bien la entidad y empresa supervisada delega sus bienes y servicios de TI a terceros, la responsabilidad sigue siendo de la entidad y en caso de materializarse riesgos en el tercero, la entidad es la que debe responder ante sus partes interesadas, por lo que la redacción de la propuesta mantiene la expectativa de alto nivel de las superintendencias para la gestión de los riesgos relacionados. Por su parte, el parrado indica que para dicha disposición se entiende por tercero	

	requerimientos de la entidades y empresas supervisadas.	a: proveedores, alianzas estratégicas, negocios conjuntos, convenios u otro tipo de arreglo comercial. Por otra parte, se modificó parte de la redacción de la disposición para mejorar el entendimiento.	
	[339]ISACA El concepto "tercerización de la información" no está definido en el escrito, ¿Qué es? Agregaría "reguladores" al final	**[339]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.	
Lo anterior incluye a 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.
Se deben establecer controles a fin de comprobar que los proveedores implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital de los bienes y servicios de TI proveídos, de conformidad con los requerimientos de la entidades y empresas supervisadas.		Se modifica la redacción para mejorar el entendimiento de la disposición.	Las entidades y empresas supervisadas ~~Se~~ 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 los bienes y servicios de TI proveídos~~, 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 estos sean subcontratados, se cuente con controles de seguridad y planes de continuidad del negocio.		Se modifica la redacción para mejorar el entendimiento de la disposición.	Cuando los bienes y servicios de TI críticos sean proveídos por terceros, las entidades y empresas supervisadas deben asegurar que, en caso de que ~~estos 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 ~~y~~ planes de continuidad del negocio.
		Se incorpora párrafo a fin de asegurar las medidas de control de seguridad de la información y seguridad cibernética cuando se delegue información confidencial o sensible a terceros.	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 bienes y servicios de TI proveídos por terceros			**Artículo 26. Identificación de bienes y servicios de TI proveídos por terceros**
Las entidades y empresas supervisadas deben establecer procedimientos que permitan mantener identificados los bienes y servicios de TI proveídos por terceros. Además, deben mantener identificados sus proveedores de bienes y servicios de TI críticos, a través de un análisis de riesgos.	**[340]MUCAP** No queda claro el alcance del análisis de riesgos, sería para todos los proveedores de bienes y servicios, o solo para los proveedores de bienes y servicios "críticos".	**[340] No procede** La disposición indica que deben mantener identificados sus proveedores de bienes y servicios de TI críticos, a través de un análisis de riesgos.	Las entidades y empresas supervisadas deben establecer procedimientos que permitan mantener 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.
	[341]CFBNCR 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.	**[341] No procede** Las entidades y empresas supervisadas deben 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.	
	[342]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	**[342]No procede** Las entidades y empresas supervisadas deben 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	

	atención a las mejores prácticas y el principio de proporcionalidad.	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.	
	[343]SEGUROSLAFISE Considerar el cambio de la redacción a: Proveedores de bienes y servicios de TI críticos: Persona física o jurídica que provee bienes o servicios de TI críticos a la entidad o empresa supervisada, indistintamente de su domicilio, incluyendo subcontratistas o asociados.	**[343] 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. Por otra parte, la definición establecida en el artículo 4 para "Proveedores de bienes y servicios de TI críticos", se modificó.	
	[344]BCR Se podría garantizar los bienes de TI que se encuentren dentro de las instalaciones del CFBCR.	**[344] No procede** No se entiende el comentario dentro del contexto de la disposición.	
	[345]ISACA El análisis de riesgos podría encapsular todo tipo de control, pero debe ser explícito el lineamiento que se refiera a la identidad del proveedor como una persona jurídica, es decir la situación financiera, su disponibilidad y capacidad para aceptar más clientes, los sistemas de control, de gobierno, de gestión, etc. del proveedor.	**[345] No procede** Las entidades y empresas supervisadas deben 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.	
		Se incorpora párrafo a fin de asegurar las medidas de control de seguridad de la información y seguridad cibernética cuando se delegue información confidencial o sensible a 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 bienes y servicios de TI críticos			**Artículo 27. Identificación, evaluación y monitoreo de los riesgos de tercerización de bienes y servicios de TI críticos**
Las entidades y empresas supervisadas deben identificar, evaluar y monitorear, de conformidad con las políticas establecidas, los riesgos de tercerización de bienes y servicios de TI críticos, así como revelar dichos riesgos en el perfil tecnológico.	**[346]CFBNCR** 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.	**[346] No procede** Las entidades y empresas supervisadas deben 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 identificar, evaluar y monitorear, de conformidad con ~~las~~ 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~~, así como~~. Además, se deben revelar dichos riesgos en el perfil tecnológico.
	[347]ABC El Reglamento debe incluir 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 las expectativas del regulador en esta materia, en atención a las mejores prácticas y el principio de proporcionalidad.	**[347] No procede** Las entidades y empresas supervisadas deben 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.	
	[348]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.	**[348] No procede** Las entidades y empresas supervisadas deben 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.	
Artículo 28. Acuerdos de confidencialidad			**Artículo 28. Acuerdos de confidencialidad**
Las entidades y empresas supervisadas que deleguen bienes y servicios de TI a terceros deben suscribir acuerdos de confidencialidad previo al intercambio de información con los proveedores.	**[349]ISACA** Este concepto debería ser sustituido por Acuerdo de No Divulgación de Información, ya que un acuerdo de confidencialidad se refiere a la información confidencial, pero las empresas utilizan otras categorías de clasificación como privada, restringida, personal, etc. Por lo que este concepto debilita el control: Como la información privada no está etiquetada como confidencial entonces ¿se puede sustraer y compartir con cualquier persona?	**[349] No procede** Los acuerdos de confidencialidad hacen referencia a la no divulgación de la información, indistintamente de la clasificación que tenga esta. Por otra parte, se modifica la redacción para mejorar el entendimiento.	Las entidades y empresas supervisadas que deleguen a terceros, bienes y servicios de TI ~~a terceros~~ que involucren el procesamiento, la transmisión o el almacenamiento de información, deben ~~suscribir~~ establecer mecanismos de control tales como los acuerdos de confidencialidad previo al intercambio de información con dichos terceros ~~los proveedores~~.
	[350]Luis Diego León Barquero	**[350] No procede**	

	No entiendo el término de contratos de adhesión con los proveedores.	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.	
	[351]BNCR ¿Los acuerdo a nivel de servicio pueden estar dentro del contrato o deben ser independientes (contrato y acuerdo)?	**[351]No procede** En el artículo 29 se amplió la disposición para señalar que los acuerdos de nivel de servicio podrán estar incluidos en los contratos, según la naturaleza del bien o servicio externalizado.	
	[352]COOPEMEP Considerar que podrían existir contratos de adhesión sobre servicios que no están en contacto con activos de información confidenciales y el texto no lo contempla.	**[352]Procede** Se ajusta la redacción de la disposición considerando parte de lo sugerido.	
	[353]FEDEAC Para contratos que no tienen o no requieren cláusula de confidencialidad, considerar que podrían existir contratos de adhesión sobre servicios que no están en contacto con activos de información confidenciales y el texto no lo contempla.	**[353]Procede** Se ajusta la redacción de la disposición considerando parte de lo sugerido.	
	[354]COOPEBANPO Considerar que podrían existir contratos de adhesión sobre servicios que no están en contacto con activos de información confidenciales y el texto no lo contempla.	**[354]Procede** Se ajusta la redacción de la disposición considerando parte de lo sugerido.	
	[355]AAP Se sugiere refrasear para incluir que estas cláusulas de acceso	**[355] Procede**	

	entran en el transitorio cuarto: Contratos con proveedores de Bienes y Servicios de TI. Se solicita aclarar que esto no incluye contratos de Adhesión, es decir que la Sugese conoce que proveedores con contratos de adhesión no firman acuerdos y que este punto solo es para instar a mantener la confidencialidad dentro de lo posible.	Se ajusta la redacción para mejorar el entendimiento de la disposición considerando parte de lo sugerido.	
	[356]SEGUROSLAFISE Favor refrasear para incluir que estas cláusulas de acceso entran en el transitorio cuarto: Contratos con proveedores de Bienes y Servicios de TI. Favor aclarar que esto no incluye contratos de Adhesión, es decir que la Sugese conoce que proveedores con contratos de adhesión no firman acuerdos y que este punto solo es para instar a mantener la confidencialidad dentro de lo posible.	**[356] Procede** Se ajusta la redacción para mejorar el entendimiento de la disposición considerando parte de lo sugerido.	
	[357]BCR Los acuerdos de confidencialidad para los contratos de adhesión serán de acuerdo con las condiciones establecidos con los terceros. Se recomienda ajustarla redacción para que contemple este caso.	**[357] Procede** Se ajusta la redacción para mejorar el entendimiento de la disposición considerando parte de lo sugerido.	
	[358]CIS Considerar que podrían existir contratos de adhesión sobre servicios que no están en contacto con activos de información confidenciales y el texto no lo contempla.	**[358]Procede** Se ajusta la redacción de la disposición considerando parte de lo sugerido.	
	[359]CCPA	**[359]No Procede**	

	Recomendamos realizar el siguiente cambio: Artículo 28. Acuerdos de confidencialidad Las entidades y empresas supervisadas que deleguen bienes y servicios de TI a terceros deben suscribir acuerdos de confidencialidad previo al intercambio de información con los proveedores. Las entidades y empresas supervisadas deben asegurar la confidencialidad de la información de acuerdo a la normativa que rija para la información contenida en los servicios y bienes de TI que se deleguen, incluso en los casos en que se celebren contratos de adhesión con los proveedores." Recomendamos además realizar un detalle de requisitos mínimos para el acuerdo de confidencialidad solicitado por el Conassif.	La redacción fue modificada a partir de lo indicado en la observación [352].	
Las entidades y empresas supervisadas deben asegurar la confidencialidad de la información incluso en los casos en que se celebren contratos de adhesión con los proveedores.		Se modifica la redacción para mejorar el entendimiento de la disposición.	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. ~~incluso en los casos en que se celebren contratos de adhesión con los proveedores.~~
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.	**[360]ISACA** Promover la separación entre el SGSI y la seguridad cibernética es caer en incumplimiento normativo internacional, esto es el principal factor crítico de éxito en la implementación de un SGSI. La seguridad cibernética es parte de la Seguridad de la Información,	**[360] No procede** El comentario de la observación no está relacionado con el contexto del artículo 29. Por otra parte, Se modifica la redacción para mejorar el entendimiento de la disposición.	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.

	no debe permitirse que exista dicha separación. Lo que si se debe aclarar es que en la Gestión de TI debe existir la función de seguridad operativa que es la ejecución de tareas y actividades aplicando el SGSI (políticas, procedimientos, herramientas, etc.). Esto debe aplicarse en los alcances de seguridad física, legal y administrativa, ya que todo debe estar bajo la gestión del SGSI.		
	[361]Luis Diego León Barquero No entiendo el término de contratos de adhesión con los proveedores.	**[361] 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.	
	[362]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 3-Debe depender del tipo de servicio, por ejemplo, para el servicio de desarrollo no necesariamente es necesario garantizar la continuidad.	**[362] 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 los contratos y acuerdos de nivel de servicio deben contener cláusulas que aseguren la continuidad de los bienes y servicios de TI tercerizados. 3-Lo indicado es parte de las actividades que las entidades y empresas supervisadas deben realizar en la implementación de la disposición de establecer procesos para gestionar los contratos y los acuerdos de nivel de servicio del artículo 29.	
	[363]MUCAP Se debe considerar y valorar que la posibilidad de negociar contratos de adhesión con empresas multinacionales es muy poca.	**[363]No procede** El artículo entre otras disposiciones indica que 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, por lo que esta disposición no se está refiriendo a la negociación de los contratos, si no a los riesgos que pueden existir.	
	[364]AAP Se solicita modificar la redacción del texto para que explique que aplica a proveedores de servicios catalogados como críticos.	**[364] No procede** La redacción indica que aplica para los proveedores de bienes y servicios de TI. Por otra parte, se incluye en la disposición que: 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.	
	[365]CFBNCR Se sugiere ajustar el párrafo 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. En algunos de los artículos de esta norma se definen que, para la gestión con los proveedores, además del contrato deben existir acuerdos de nivel deservicio (SLA), lo cual impacta los procesos de adquisición, ya que en la actualidad los acuerdos de nivel de servicio o SLA están inmersos formalmente dentro de las cláusulas establecidas a nivel de contrato y no son tratados de manera independiente, por lo que se agradece analizar este tema y valorar el ajuste en el artículo. Así mismo, a la empresa o profesional independiente que realice la auditoría externa de TI,	**[365]No procede** Se modifica la redacción y se acota la disposición a bienes y servicios de TI críticos que son tercerizados. Por otra parte, se amplió la disposición para señalar que los acuerdos de nivel de servicio podrán estar incluidos en los contratos, según la naturaleza del bien o servicio externalizado.	

	debe garantizar que su labor no interfiera con las operaciones para la prestación de los servicios de la entidad o empresa supervisada".		
	[366]ABC En el caso de las entidades públicas, sujetas a la ley de contratación administrativa, debe considerarse que los acuerdos de nivel de servicio forman parte de las cláusulas contractuales, por lo que la redacción debería dar cobertura a esta particularidad.	**[366] Procede** Se amplió la disposición para señalar que los acuerdos de nivel de servicio podrán estar incluidos en los contratos, según la naturaleza del bien o servicio externalizado.	
	[367]SMSEGUROS Considerar la redacción del texto para que esto aplique a proveedores de servicios catalogados como críticos.	**[367] No procede** La redacción indica que aplica para los proveedores de bienes y servicios de TI. Por otra parte, como parte de la disposición se agregó que 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.	
	[368]SEGUROSLAFISE Favor, modificar la redacción del texto para que explique que aplica a proveedores de servicios catalogados como críticos.	**[368] No procede** La redacción indica que aplica para los proveedores de bienes y servicios de TI. Por otra parte, como parte de la disposición se agregó que 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.	
	[369]COOPENAE (Impacto Bajo, Esfuerzo Medio) Representa requerimientos detallados que modifican el proceso actual de gestión, de acuerdo con niveles de servicio.	**[369] No procede** El articulo incluye entre otras disposiciones que las entidades y empresas supervisadas deben considerar para el diseño de los contratos y acuerdos de nivel de servicio los aspectos que están establecidos en los lineamientos generales del presente reglamento.	
	[370]BCR	**[370] No procede**	

	Esto no procede, dado que en los contratos de adhesión no se contratan bienes en general, se contratan servicios. Los bienes están fuera del ámbito legal del contratante.	La naturaleza de los negocios es muy cambiante, por lo tal, la disposición incluye bienes y servicios, en caso de que estos fuesen a llegar a ser incluidos como parte de los contratos de adhesión.	
	[371]ISTMO Primer párrafo, debe limitarse a proveedores de servicios críticos, así como está la redacción se entiende que es para todos, inclusive servicios no críticos. Adicionalmente considerar que los grandes proveedores del mundo y líderes en la industria no van a firmar un SLA con formatos específicos, ellos ya poseen sus propios acuerdos y son de adhesión, previo a la contratación uno los acepta y listo, sino no se usan. Pero formatos particulares no los firman. Considerar cambio en la redacción de este artículo.	**[371] No procede** La redacción indica que aplica para los proveedores de bienes y servicios de TI. Por otra parte, como parte de la disposición se agregó que 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. Por otra parte, se adicionó a la disposición lo siguiente: Mediante lineamientos generales del presente reglamento se establecen elementos a considerar para el diseño de los contratos y acuerdos de nivel de servicio, salvo que se trate de bienes o servicios suministrados por proveedores de computación en la nube o contratos de adhesión.	
	[372]CCPA Recomendamos realizar cambios contemplando lo indicado en la respuesta al artículo 28.	**[372] No procede** Se consideró para la modificación de la disposición parte de la observación [352]	
Los contratos y acuerdos de nivel de servicio deben contener cláusulas que aseguren la continuidad de los bienes y servicios de TI tercerizados.	**[373]COOPEBANPO** Las cláusulas para asegurar la continuidad deberían considerarse solo para proveedores que brinden bienes y servicios críticos, ya que pedir continuidad para un servicio que no tiene afectación para la empresa, podría ser abusivo y hasta oneroso para la entidad.	**[373] Procede** Se modifica la redacción con parte de lo señalado en la observación.	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.
	[374]OPC-CCSS En materia de adquisición de bienes no se celebran acuerdos de	**[374] No procede** La naturaleza de los negocios es muy cambiante, por lo tal, la disposición	

	niveles de servicio dado que la adquisición de bienes se da por una vez en un momento determinado de tiempo, esto quiere decir que la relación comercial puede acabar al momento de entrega del bien y dar por ejemplo la garantía mediante el fabricante del bien, no necesariamente mediante el proveedor que suministró el bien.	incluye bienes y servicios, en caso de que estos fuesen a llegar a ser incluidos como parte de los contratos de adhesión.	
	[375]CB En cuanto al párrafo segundo, se sugiere ajustar el párrafo 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, 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". Asimismo, se sugiere al Regulador valorar incluir en los contratos, las evaluaciones a los proveedores para verificar los cumplimientos en materia de ciberseguridad y gestión de riesgos. En cuanto al tema de continuidad, debe depender del tipo de servicio, por ejemplo, para el servicio de desarrollo no necesariamente es necesario garantizarla continuidad. En cuanto al párrafo último, se debe tener en cuenta, según lo apuntado en	**[375] No procede** Como parte de la disposición se agregó que 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. En relación con lo señalado sobre auditoría, se considera que es un asunto que no forma parte de lo que busca la disposición reglamentaria.	

	disposiciones anteriores que la posibilidad de negociar contratos de adhesión con empresas multinacionales es muy poca, por no decir ninguna.		
Los elementos que se deben considerar para el diseño de los contratos y acuerdos de nivel de servicio están establecidos en los lineamientos generales del presente reglamento.		Se modifica la redacción para mejorar el entendimiento de la disposición.	Las entidades y empresas supervisadas deberán diseñar sus ~~Los elementos que se deben considerar para el diseño de los~~ contratos y acuerdos de nivel de servicio ~~están establecidos en los~~ 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, a través de los contratos y los acuerdos de nivel de servicio, que las Superintendencias tengan acceso a los registros, datos e información de los bienes y servicios de TI tercerizados.	**[376]ISACA** Se indica que el programa se establece anualmente y en función de los riesgos, precisamente los mismos riesgos que tienen todos los servicios financieros. Las pruebas de vulnerabilidades deben ser aplicadas en varios momentos del año, de forma trimestral y en cambios significativos, referidos a cualquier elemento o componente de TIC. Las pruebas deben incluir análisis de vulnerabilidades, y pentesting de varios sabores.	**[376] No procede** La disposición del artículo no incluye los aspectos indicados en la observación.	Las entidades y empresas supervisadas deben asegurar, ~~a través de los contratos y los acuerdos de nivel de servicio,~~ que las Superintendencias tengan acceso a los registros, datos e información de los bienes y servicios de TI tercerizados según sean requeridos como parte de los procesos de supervisión.
	[377]Luis Diego León Barquero	**[377] No procede**	

	No entiendo el término de contratos de adhesión con los proveedores.	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.	
	[378]BPDC Esto tiene implicaciones contractuales, se debe valorar 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 ley 9048. Además, hay que considerar que el contrato de adhesión no se puede modificar para incluir esa condición, lo que sí se puede hacer es crear un usuario con los privilegios para poder tener acceso a la información y ese usuario entregárselo a la superintendencia	**[378] Procede** Se modifica la redacción con parte de lo señalado en la observación	
	[379]COOPEANDE En este tema cuando se trata de fabricantes de clase mundial que los contratos ya son estándar y es muy complejo que estas organizaciones permitan ajustes a los mismos para incluir lo que se está solicitando en este artículo. Sin embargo, este tipo de proveedores poseen mecanismos e informes que permiten validar el desempeño, la seguridad y la calidad del servicio.	**[379] Procede** Se modifica la redacción con parte de lo señalado en la observación	
	[380]JUPEMA	**[380] Procede**	

	No es claro el artículo, ¿Se debe dar acceso al ente regulador a la información que se tiene en la nube? En caso de ser así, ¿con qué fin? ¿Qué medidas de seguridad se le aplicará al regulador para el acceso?	La redacción fue modificada para mejorar el entendimiento.	
	[381]COOPEMEP Considerar establecer a grandes rasgos como la superintendencia va a hacer solicitud de los accesos pues se podría entender que solo se necesita un acceso de este nivel en caso de procesos de intervención o judiciales, pero no parece correcto que el regulador solicite bases de datos para validar si ya tiene un mecanismo de solicitud de información que puede utilizar.	**[381] No procede** La redacción fue modificada para mejorar el entendimiento.	
	[382]FEDEAC En este tema cuando se trata de fabricantes de clase mundial que los contratos ya son estándar y es muy complejo que estas organizaciones permitan ajustes a los mismos para incluir lo que se está solicitando en este artículo. Sin embargo, este tipo de proveedores poseen mecanismos e informes que permiten validar el desempeño, la seguridad y la calidad del servicio. No es claro el artículo, ¿se debe dar acceso al ente regulador a la información que se tiene en la nube?, si es así, ¿con qué fin y qué medidas de seguridad se le aplicará al regulador para el acceso? En el caso de los contratos de adhesión con los proveedores se debe especificar si el acceso de las	**[382] Procede** La redacción fue modificada para mejorar el entendimiento.	

	Superintendencias se pretende hacer a través de la entidad, con usuarios controlados por la entidad supervisada o ¿de qué forma? Se debe establecer que la superintendencia va a tener acceso a la información con un usuario administrado por la entidad, pues se podría entender que solo se necesita un acceso de este nivel en caso de procesos de intervención o judiciales, pero no parece correcto que el regulador solicite bases de datos para validar si ya tiene un mecanismo de solicitud de información que puede utilizar.		
	[383]COOPEBANPO Considerar establecer a grandes rasgos como la superintendencia va a hacer solicitud de los accesos pues se podría entender que solo se necesita un acceso de este nivel en caso de procesos de intervención o judiciales, pero no parece correcto que el regulador solicite bases de datos para validar si ya tiene un mecanismo de solicitud de información que puede utilizar. El acuerdo debería establecer tácitamente que los accesos son para sus actividades de supervisión. Así como queda, le estaría dando atribuciones que no le competen, pues no lo dices específicamente.	**[383] Procede** La redacción fue modificada para mejorar el entendimiento.	
	[384]AAP Se solicita incluir en la redacción que estas cláusulas de acceso aplican igual dentro de la disposición transitoria cuarta: Contratos con proveedores de	**[384] No procede** La redacción fue modificada para mejorar el entendimiento.	

	Bienes y Servicios de TI. Ampliar cómo sería el procedimiento para la solicitud del acceso a la información.		
	[385]BAC De acuerdo con lo indicado en la sesión del 13 de diciembre 2023 con los reguladores, se solicita modificar la redacción de este artículo para que quede claro que los accesos a los que se hace referencia son requeridos "por demanda", ya sea por una visita en sitio o por un requerimiento específico. Que no se trata de accesos permanentes.	**[385]Procede** La redacción fue modificada para mejorar el entendimiento.	
	[386]ABC La norma debe aclarar que estos accesos son “por demanda” y no permanentes.	**[386] No procede** La redacción fue modificada para mejorar el entendimiento.	
	[387]CB En el mismo sentido que comentamos en el artículo 29, dependiendo del contrato de adhesión esto no sería posible de forma directa, sino que la empresa supervisada deberá darle acceso a la Superintendencia a su instancia para que pueda hacer las supervisiones del caso. Es importante considerar esta situación y que se realicen los ajustes necesarios en la norma para adaptarla a la realidad existente.	**[387] Procede** La redacción fue modificada para mejorar el entendimiento.	
	[388]SEGUROSLAFISE Favor incluir que estas cláusulas de acceso aplican igual dentro de la disposición transitoria cuarta: Contratos con proveedores de Bienes y Servicios de TI. Ampliar	**[388] No procede** La redacción fue modificada para mejorar el entendimiento.	

	cómo sería el procedimiento para la solicitud del acceso a la información.		
	[389]BCR • Se solicita aclaración, por cuanto se podría interpretar que se requiere acceso a datos confidenciales o privados que podría ir en detrimento de la protección de estos – mecanismos e infraestructura que son utilizados para su protección. • ¿Qué sucede si los proveedores ponen algunos límites en la información a los cuales dan acceso? ¿A qué registros, datos e información de los bienes y servicios tercerizados, es que las superintendencias desean tener acceso? • ¿Qué sucede si los proveedores ponen algunos límites en la información a los cuales dan acceso? • ¿A qué registros, datos e información de los bienes y servicios tercerizados, es que las superintendencias desean tener acceso? • Se solicita que por parte de las Superintendencias se realice una validación del alcance legal de lo solicitado.	**[389] Procede** La redacción fue modificada para mejorar el entendimiento.	
	[390]CIS Considerar establecer a grandes rasgos como la superintendencia va a hacer solicitud de los accesos pues se podría entender que solo se necesita un acceso de este nivel en caso de procesos de intervención o judiciales, pero no parece correcto	**[390] Procede** La redacción fue modificada para mejorar el entendimiento.	

	que el regulador solicite bases de datos para validar si ya tiene un mecanismo de solicitud de información que puede utilizar.		
	[391]ISTMO Difícilmente que esto quede explícito en contratos de adhesión cuando se trata de servicios de nube pública (Azue, AWS, OCI, Google, etc). Sin embargo, el artículo 23, inciso h establece que la gestión de usuarios debe quedar en poder de la organización, con lo cual se puede asegurar y brindar accesos al regulador en caso de que sean requeridos. Considerar que la redacción más bien esté alineada a lo establecido en el artículo 23 y que es responsabilidad y obligación de la empresa regulada la gestión y accesos al regulador.	**[391] No procede** La redacción fue modificada para mejorar el entendimiento.	
	[392]CCPA Recomendamos realizar cambios contemplando lo indicado en la respuesta al artículo 28.	**[392] No procede** No proceden los cambios solicitados en el artículo 28, según lo resuelto en la observación [359]	
	[393]ISACA Con el propósito de evitar que esto se entienda como una "conectividad directa" a los registros datos de una base de datos y que esto le traslade al supervisor u organismo auditor responsabilidades en cuanto a la aplicación y efectividad de controles que garanticen la seguridad o privacidad de los datos en dicha conectividad, se podría mejorar la redacción para indicar "...deben garantizar la disposición y el acceso a los	**[393] Procede** La redacción fue modificada para mejorar el entendimiento.	

	registros, datos e información requerida por las Superintendencias para poder ejercer sus labores de supervisión, sin ningún tipo de restricción o condición requerida en los bienes o servicios de TI tercerizados, incluyendo aquellos 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.			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 cibernética del presente reglamento.	**[394]Luis Diego León Barquero** No entiendo la separación que este reglamento hace entre la seguridad de la información y la seguridad cibernética. Tampoco entiendo el concepto de seguridad digital.	**[394] 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.	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.
	[395]BPDC Se debe clarificar si el SGSI debe ser certificado o no, en caso de requerirlo dar tiempo prudencia	**[395] No procede** Las superintendencias requieren que las entidades y empresas supervisadas diseñen, implementen, mantengan y monitoreen un sistema de gestión de la seguridad de la información que incluya las disposiciones de seguridad cibernética del presente reglamento.	

		Las decisiones de certificar el SGSI, queda a discreción de cada entidad o empresa supervisada en función de su estrategia de negocio.	
	[396]MUCAP La norma no está clara en cuanto a si la Declaración de aplicabilidad debe ser revelada o es un documento interno; por lógica y de acuerdo a la normativa debería ser confidencial de no acceso a terceros; lo contrario daría ventajas de un ataque cibernético por la información que contiene.	**[396] Procede** Se ajusta la redacción para aclarar el entendimiento de la disposición.	
	[397]FEDEAC Valorar si los Lineamientos de este Reglamento deben detallar un marco de referencia aplicable al sistema de gestión. ¿Las superintendencias van a definir el Marco de referencia en los lineamientos o cada entidad aplicará los estándares internacionales, mejores prácticas, etc. que prefieran? ¿Con qué marco va a evaluar este punto el supervisor o auditor externo?	**397] No procede** La disposición indica que, 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.	
	[398]OPC-CCSS 1. A lo largo del RGGTI se mencionan las nuevas responsabilidades en cuanto a la seguridad de la información y seguridad cibernética, lo cual implicará costos en recurso humano, tecnología y tiempo para su cumplimiento. ¿Qué sucede con las empresas que operan al costo, se podrá implementar esto de forma gradual? ¿Habrá algún tipo de ayuda por parte de algún ministerio (como MICITT) para	**[398]No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	

	esto? ¿Capacitaciones por parte de los supervisores?2. Se menciona como parte de los antecedentes del reglamento que el mismo está soportado por la regulación basada en riesgos, sin embargo, se otorga potestad a las superintendencias de requerir la inclusión de prácticas y controles de seguridad con lo cual sería contradictorio el modelo de análisis del apetito de riesgo que al respecto haya definido la entidad.		
	[399]COOPENAE Si bien es cierto el tema de Ciberseguridad es crucial, el llegar a implementar un proceso sólido y bajo estándares y certificaciones internacionales, se requiere esfuerzo e inversión económica; asimismo, es importante tomar en cuenta el nivel de madurez y profundización que cuente cada entidad en temas de banca digital. Debido a esto, consideramos oportuno definir una gradualidad y un tiempo prudencial para poder implementar dicho proceso, basada en esa madurez digital. En la actualidad, el sector cooperativo incorpora instituciones financieras que son lo bastante maduras a nivel digital y su volumen de negocio digital representa también un componente clave, con respecto a otras instituciones, cuyo modelo de negocio pudiese ser menos intenso. En virtud de lo anterior, consideramos clave definir esa gradualidad en al menos 36 meses, basado entre otras cosas, en el tamaño de cada	**[399]No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	

	cooperativa, su modelo de negocio, así como en su nivel de digitalización y de puntos de control del riesgo tecnológico.		
	[400]ISACA Es reiterada la observación de dejar fuera de lo explícito a la seguridad legal, administrativa y física.	**[400] No procede** La gestión de riesgos se debe realizar de forma integral en la organización.	
El sistema de gestión de la seguridad de la información debe establecer los controles que permitan adoptar un enfoque basado en el riesgo, para proteger los activos de información y los activos que soportan la información, contra los riesgos de la seguridad de la información y la seguridad cibernética. Los controles deberán ser revelados mediante una declaración de aplicabilidad y especificar los atributos que están establecidos en los lineamientos generales del presente reglamento.		Se modifica la redacción para mejorar el entendimiento de la disposición.	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 ~~revelados mediante~~ una declaración de aplicabilidad y especificar los atributos que están establecidos en los lineamientos generales del presente reglamento.
Para la implementación del sistema de gestión de la seguridad de la información, se pueden utilizar los estándares internacionales, mejores prácticas o marcos de referencia relacionados con la seguridad de la información y la seguridad cibernética que la industria de tecnologías ha desarrollado.			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.	**[401]CB** Se solicita que en la norma se aclare cómo se comunicarán esos requisitos y cómo se establecerán los criterios para dar cumplimiento adecuado a las mismas.	**[401] No procede** Estas solicitudes se realizarán como parte de las labores de supervisión de TI, de cada una de las superintendencias.	Las Superintendencias podrán requerir la inclusión de prácticas y controles de seguridad de la información y seguridad cibernética dentro del sistema de gestión de la seguridad de la información de acuerdo con las necesidades de supervisión y el riesgo identificado.
Artículo 32. Seguridad cibernética			**Artículo 32. Seguridad cibernética**
Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital. Además, deben establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	**[402]Luis Diego León Barquero** No entiendo la separación que este reglamento hace entre la seguridad de la información y la seguridad cibernética. Tampoco entiendo el concepto de seguridad digital.	**[402] No procede** **P**ara 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**.**	Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital. ~~Además, deben establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.~~

	[403]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?	**[403] No procede** Seguridad Cibernética y Ciberseguridad se utilizan de forma indistinta, para efectos del presente Reglamento se utiliza 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.	
	[404]COOPEANDE Este artículo es un poco confuso, ya que la seguridad de la información como sistemas de gestión incluye la seguridad tecnológica y la ciberseguridad. El que la entidad tenga un área que gestione la seguridad de la información y otra que aplique los controles a nivel de seguridad de Ti y Ciberseguridad no sustituye que la seguridad de la información es la que emite el gobierno y las políticas. Lo que podría generar este artículo es que se vean como procesos separados y que la seguridad de la información tenga pierda ese enfoque transversal.	**[404] Procede** Se modificó la redacción de la disposición para mejorar el entendimiento. Se eliminó lo referente a establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	
	[405]JUPEMA Se solicita más claridad del concepto de separación, pues hay ambigüedad en la redacción.	**[405] Procede** Se modificó la redacción de la disposición del artículo para mejorar el entendimiento. Se eliminó lo referente a establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	
	[406]FEDEAC Este artículo es un poco confuso, ya que la seguridad de la	**[406] Procede** Se modificó la redacción de la disposición del artículo para mejorar el	

	información como sistemas de gestión incluye la seguridad tecnológica y la ciberseguridad. El que la entidad tenga un área que gestione la seguridad de la información y otra que aplique los controles a nivel de seguridad de Ti y Ciberseguridad no sustituye que la seguridad de la información es la que emite el gobierno y las políticas. Lo que podría generar este artículo es que se vean como procesos separados y que la seguridad de la información pierda ese enfoque transversal. Se solicita más claridad del concepto de separación, pues hay ambigüedad en la redacción.	entendimiento. Se eliminó lo referente a establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	
	[407]CAJAANDE Pregunta ¿A qué se refieren con que la seguridad cibernética esté integrada o separada del SGSI? Por definición, la seguridad cibernética forma parte del alcance de la gestión de seguridad de la información. A nivel institucional se cuenta con una unidad de seguridad de la información que emite directrices a nivel de gobierno y también ha implementado un SGSI con las disposiciones que a nivel técnico se deben cumplir para resguardar la confidencialidad, integridad y disponibilidad de la información, el Departamento de TI se encarga de implementar dichos controles de manera alineada con las directrices. En algunos casos la Unidad de Seguridad de la información también realiza	**[407]No Procede** Se modificó la redacción de la disposición del artículo para mejorar el entendimiento. Se eliminó lo referente a establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	

	funciones a nivel de gestión en la implementación de algunos controles Al indicar “establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información” ¿a qué se refieren puntualmente?		
	[408]CFBNCR 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.	**[408] No procede** Este artículo trata únicamente sobre la seguridad cibernética.	
	[409]CB Se sugiere cambiar el término “Seguridad Cibernética” por “Ciberseguridad” que es más conocido y utilizado.	**[409] No procede** Seguridad Cibernética y Ciberseguridad se utilizan de forma indistinta, para efectos del presente Reglamento se utiliza 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.	
	[410]COOPENAE	**[410] No Procede**	

	(Impacto Alto, Esfuerzo Alto) Profundiza significativamente en las actividades de ciberseguridad. No solicita una estructura de organización específica para este tema, pero por su alcance de actividades, será necesario abordarlo, sea de forma interna, o subcontratado.	Se modificó la redacción de la disposición para mejorar el entendimiento. Adicionalmente, se amplía el ámbito del articulo 34	
	[411]ISACA Es reiterada la observación de dejar fuera de lo explícito a la seguridad legal, administrativa y física.	**[411] No procede** La gestión de riesgos debe de realizarse de forma integral en la organización.	
En caso de que la seguridad cibernética esté integrada, los controles deben estar identificados. Si está separada, se deben diseñar, implementar y monitorear los principios, políticas y procedimientos, así como establecer los presupuestos, las tecnologías, la formación y el recurso humano necesarios para gestionar el riesgo de la seguridad cibernética.		Se eliminó el párrafo según lo atendido en la observación [406]: Se modificó la redacción de la disposición del artículo para mejorar el entendimiento. Se eliminó lo referente a establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	~~En caso de que la seguridad cibernética esté integrada, los controles deben estar identificados. Si está separada, se deben diseñar, implementar y monitorear los principios, políticas y procedimientos, así como establecer los presupuestos, las tecnologías, la formación y el recurso humano necesarios para gestionar el riesgo de la seguridad cibernética.~~
Las entidades y empresas supervisadas deben establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética.			Las entidades y empresas supervisadas deben establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética.
Artículo 33. Programas de análisis de vulnerabilidades y pruebas			
Las entidades y empresas supervisadas deben establecer, anualmente, programas de análisis de vulnerabilidades y pruebas que incluyan los controles de seguridad de la información y seguridad cibernética.	**[412]Luis Diego León Barquero** Estoy de acuerdo con ejecutar programas de análisis de vulnerabilidades y pruebas. Sin embargo, no entiendo la separación que este reglamento hace entre la seguridad de la información y la seguridad cibernética.	**[412] No procede** Para las Superintendencias es relevante destacar el tema de la seguridad cibernética. 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.	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.
	[413]FEDEAC Valorar si se requiere mayor detalle sobre los alcances o	**[413] No procede** La gestión de riesgos debe de realizarse de forma integral en la organización, por	

	estándares de los programas de análisis. ¿El ente regulador va a definir los lineamientos para este punto, de tal forma que el requerimiento no sea tan genérico y la expectativa del regulador no difiera de las pruebas realizadas?	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.	
	[414]ABC El reglamento menciona análisis de vulnerabilidades y pruebas, pero no especifica claramente qué tipos de pruebas (como pruebas de penetración -pentesting-, auditorías de seguridad, simulaciones, etc.) son requeridas. Adicionalmente, en los lineamientos generales no se aclara nada al respecto. Es necesario que se especifique o proporcione ejemplos de los tipos de pruebas consideradas adecuadas para cumplir con el reglamento, las cuales deben ser razonables y cuya realización sea esporádica, y que no impliquen un costo desproporcionado. De acuerdo con la norma, las pruebas pueden ser realizadas por personal interno. Según lo anterior, ¿los test de penetración realizados por terceros son opcionales?	**[414] No procede** La gestión de riesgos debe de 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.	
	[415]COOPENAE (Impacto Alto, Esfuerzo Alto) Desde la perspectiva de ciberseguridad, en el Anexo 4 “Funciones para la evaluación de riesgos de Seguridad Cibernética” se incluyen pautas que resumen un marco de gestión de ciberseguridad llamado “NIST Cibersecurity Framework”.	**[415] Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	

	Este marco es un equivalente de "COBIT", con orientación a ciberseguridad, mientras que COBIT tiene una orientación hacia gobierno de tecnología. Esto implica, entre otras cosas definir entre otros, estructura organizacional, roles y capacitación. Asimismo, se requerirá gradualidad para crear la madurez y el "expertise" de los recursos asignados a estos temas. Esta norma ocasiona la necesidad de evaluar el alcance de controles a desarrollar, extender las funciones del equipo de seguridad, sea de forma interna o externa e implementar herramientas para su gestión. Por otra parte, el reporte de incidentes que deben hacer las entidades por los canales oficiales a los reguladores es un cambio significativo y estas deben ser diligentes y cuidadosos con la información a reportar, clarificando los eventos, la forma como se reportan, sea en línea o fuera de línea, e involucrar temas de fraude o solo de hackeo. Actualmente las entidades reportan no tener incidentes de seguridad, pero se carece de controles para su detección. En la norma en consulta se fortalece la detección para así poder llegar a la gestión de incidentes. Si se trabaja en protección, eso disminuye la probabilidad de incidentes y por ende la necesidad		

	de reportarlos. Esto implica implementar una gestión completa de ciberseguridad, lo cual implica no solo herramientas, sino competencias técnicas, diseñar, implementar y gestionar controles, entre otras; asimismo definir un apetito al riesgo que permita definir la madurez a alcanzar.		
	[416]ISACA Es reiterada la observación de dejar fuera de lo explícito a la seguridad legal, administrativa y física. Aclararía específicamente si se refiere a "pruebas de intrusión" o "pruebas de control" en general	**[416] No procede** La gestión de riesgos debe de realizarse de forma integral en la organización por 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.	
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.	**[417]CB** En relación con esta disposición, se solicita aclarar si los test de penetración realizados por terceros serán opcionales.	**[417] No procede** No se hace referencia a que las entidades deban cumplir con test de penetración realizados por terceros; decidir realizar ese tipo de test es algo que queda a discreción de la entidad. La disposición indica: 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 seguridad cibernética		Se modifica el texto como parte de los comentarios de la observación [418]	**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	**[418]Luis Diego León Barquero** Creo que es necesario cambiar el párrafo siguiente: “Las entidades y	**[418] Procede** Se modifica la disposición con parte de lo señalado en la observación. Se amplía	Las entidades y empresas supervisadas deben establecer unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen los riesgos

operaciones o comités técnicos que gestionen los riesgos de la seguridad cibernética.	empresas supervisadas deben establecer unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen los riesgos de la seguridad cibernética. “Mi sugerencia sería la siguiente: 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, incluyendo la seguridad cibernética. El cambio propuesto está en negrita, tachado y subrayado.	el alcance del artículo en su epígrafe y texto con “riesgos de seguridad de la información”.	de la seguridad de la información y de la seguridad cibernética.
	[419]BPDC Se debe sugerir donde deberían estar ubicados o reportar estas unidades, funciones, centros de operación y comités.	**[419] 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 seguridad cibernética, adicionalmente, el Articulo 8 indica que el Órgano de dirección es el responsable de aprobar las estructuras necesarios para la implementación del marco de gobierno y gestión de TI.	
	[420]FEDEAC ¿El ente regulador va a definir los lineamientos para este punto, de tal forma que el requerimiento no sea tan genérico y la expectativa del regulador no difiera de las pruebas realizadas?	**[420] No procede** La observación no está dentro del contexto del artículo 34 ya que este no se refiere a pruebas, además, cabe destacar que la gestión de riesgos dentro de las organizaciones, deben de realizarse de forma integral en la organización por 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.	
	[421]VIDAPLENA ¿Puede el Área de Ciberseguridad de acuerdo con este artículo seguir formando parte de la estructura organizacional de la división, departamento o área deTI? De acuerdo con lo que se indica en el artículo, se entiende que el área de ciberseguridad puede estar junta o separada del área de Seguridad de la Información. A partir de lo anterior, se le solicita la aclaración; considerando lo que se ha indicado para el Área de Seguridad de la Información; la cual, se ha señalado en reiteradas ocasiones que no debe formar parte de la estructura organizacional de TI. Ahora si el Área de Ciberseguridad al igual que el Área de Seguridad de Información no puede formar parte directa de la estructura de la División, Dirección o Departamento de Tecnologías de la Información, la siguiente consulta. ¿Puede el área de Ciberseguridad formar parte de la estructura de la segunda o tercera línea de defensa? Por ejemplo, ser parte de la Dirección de Riesgos. Sería importante definir con mayor claridad donde podría estar ubicada el área de Ciberseguridad dentro de la estructura de la empresa, ya sea como unidad o área , que lo gestione e incluso esto aplica para la misma Área de Seguridad de la Información; dado	**[421] No Procede** La disposición indica, entre otros aspectos, que las unidades, funciones organizacionales, centros de operación y comités técnicos 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.	

	que esta última tampoco necesariamente se ha reglamentado, lo que ha generado tensión sobre su ubicación en la estructura organizacional de las áreas y hasta con la misma superintendencia, porque no hay normativa que lo defina, sino más bien se ha señalado como parte de las mejores prácticas o para evitar conflictos de interés con el Área de TI.		
	[422]ABC 1-Los Centros de Operaciones de Ciberseguridad son costosos, por lo que se solicita un plazo prudencial para su constitución progresiva. 2-No resulta claro de la norma si las entidades pueden integrar la gestión dentro de la organización de la seguridad de la información o si deben mantener separadas ambas gestiones, aunque estén integrados dentro de las funciones de SI.	**[422] Procede** 1-Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias 2-Se modificó el articulo 32 para aclarar lo indicado en esta observación.	
	[423]CB Este tipo de unidades suelen ser costosas. Por lo tanto, se solicita al Regulador un plazo prudencial para su constitución progresiva, de manera que no sea una obligación de cumplimiento inmediato.	**[423] Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias	
	[424]BCR Por favor clarificar si la gestión de seguridad cibernética y la gestión de la seguridad de la información pueden o deben ser funciones organizacionales separadas a nivel de estructura organizacional, que se complementen e integren en la	**[424] No Procede** La disposición indica, entre otros aspectos, que 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	

	práctica u operación. Esto considerando que a nivel del documento y lineamientos se habla de la gestión de ambos temas por separado; incluso detallando funciones, actividades o responsabilidades que suponen para cada caso el establecimiento de un gobierno claro y formal a cada gestión (gestión de la seguridad de la información y gestión de la seguridad cibernética).	información de las entidades o empresas supervisadas, tercerizadas o separadas. Por otra parte, en el artículo 32 se eliminó lo referente a establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.	
	[425]ISACA Es reiterada la observación de dejar fuera de lo explícito a la seguridad legal, administrativa y física.	**[425] No procede** La gestión de riesgos debe de realizarse de forma integral en la organización por 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 unidades, funciones organizacionales, centros de operaciones o comités técnicos deben establecerse de conformidad con la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por las entidades o empresas supervisadas. Además, pueden estar integrados a las áreas o funciones de seguridad de la información de las entidades o empresas supervisadas, tercerizadas o separadas.			Las unidades, funciones organizacionales, centros de operaciones o comités técnicos deben establecerse de conformidad con la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por las entidades o empresas supervisadas. ~~Además, pueden estar integrados a las áreas o funciones de seguridad de la información de las entidades o empresas supervisadas, tercerizadas o separadas.~~
		Se modificó la redacción de la disposición del artículo para mejorar el entendimiento y según lo indicado en las observaciones.	Las unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestiones los riesgos de seguridad cibernética pueden estar integrados a las áreas o funciones de seguridad de la información de las entidades o empresas supervisadas, tercerizadas o separadas
En todo caso, deben establecerse las políticas y los procedimientos que definan los propósitos, responsabilidades, actividades y controles requeridos para su operación.			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.	**[426]Luis Diego León Barquero** Se debe hablar de la seguridad de la información, pues la seguridad cibernética es parte de la seguridad de la información.	**[426] No procede** Para las Superintendencias es relevante destacar el tema de la seguridad cibernética. 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.	Las entidades y empresas supervisadas deben diseñar e implementar, anualmente, planes de promoción de la cultura de la seguridad de la información y la seguridad cibernética.
Los planes deben incluir, al menos, actividades de capacitación, concientización, divulgación, comunicación y promoción de una cultura organizacional de seguridad de la información y seguridad cibernética dirigidos a sus colaboradores, clientes, proveedores y demás partes interesadas.	**[427]COOPEANDE** Se indica que los planes de capacitación y concientización internos deben estar dirigidos también a proveedores y demás partes interesadas. Este alcance es muy amplio, y por temas de capacidad instalada y optimización de recursos esos planes de concientización se le pueden solicitar a los mismos proveedores como parte de los requisitos de cumplimiento.	**[427] Procede** Se modificó la disposición para aclarar lo indicado en la observación. Se excluyó lo referente a proveedores.	Los planes deben incluir, al menos, actividades de capacitación, concientización, divulgación, comunicación y promoción de una cultura organizacional de seguridad de la información y seguridad cibernética dirigidos a sus colaboradores, clientes~~, proveedores~~ y demás partes interesadas.
	[428]FEDEAC Aunque las Cooperativas de ahorro y crédito bajo el Acuerdo SUGEF 25-23 podrán aplicar de forma proporcional y diferenciada este artículo, se debería velar por que no haya una flexibilización extrema o aplicación nula del concepto aquí establecido. Los planes de capacitación y concientización internos cada entidad debe elaborarlos de acuerdo con su perfil de riesgo, apetito de riesgo, estrategia, por	**[428] Procede** Se modificó la disposición para aclarar lo indicado en la observación.	

	loque no debe solicitarse planes para entes externos como proveedores y otras partes interesadas.		
	[429]AAP Se solicita aclarar que no es responsabilidad de los supervisados si los proveedores/clientes eligen no hacer los cursos o la cultura y sería suficiente con una divulgación.	**[429] Procede** Se excluyó de la disposición lo referente a proveedores.	
	[430]ABC El ámbito de cobertura de esta política debería limitarse a los colaboradores y el personal de proveedores que laboren internamente en la entidad.	**[430] Procede** Se excluyó de la disposición lo referente a proveedores.	
	[431]OPC-CCSS El capítulo I, Artículo 35, párrafo 2 indica: "Los planes deben incluir, al menos, actividades de capacitación, concientización, divulgación, comunicación y promoción de una cultura organizacional de seguridad de la información y seguridad cibernética dirigidos a sus colaboradores, clientes, proveedores y demás partes interesadas". Dada la redacción del párrafo se interpreta que dicho plan debe incluir actividades de capacitación dirigidas a los proveedores de parte de la entidad contratante, es decir, ¿son las entidades supervisadas quienes deben dar esas capacitaciones a sus propios proveedores?, de no ser así se debe considerar una mejora en la redacción del párrafo para ese artículo.	**[431] Procede** Se excluyó de la disposición lo referente a proveedores.	

	[432]SEGUROSLAFISE Favor aclarar que no es responsabilidad de los supervisados si los proveedores/clientes eligen no hacer los cursos o la cultura y sería suficiente con una divulgación.	**[432] Procede** Se excluyó de la disposición lo referente a proveedores.	
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 cibernética		Se modifica la redacción para incluir referencia a seguridad de la información	**Sección II. Incidentes de seguridad de la información y seguridad cibernética**
Artículo 36. Gestión de incidentes de seguridad cibernética			**Artículo 36. Gestión de incidentes de seguridad e la información y seguridad cibernética**
Las entidades y empresas supervisadas deben diseñar e implementar un proceso para la gestión de incidentes de seguridad cibernética que incorpore las fases de la gestión de incidentes establecidas en los lineamientos generales del presente reglamento.	**[433]Luis Diego León Barquero** El marco de Gobierno y gestión de TI de COBIT 2019 tiene un objetivo de Gestionar incidentes, pero no hace distinción entre incidentes de seguridad de la información e incidentes de seguridad cibernética. De acuerdo con COBIT 2019, todos los incidentes deben ser tratados de la misma manera. Puede ser necesario clasificar los incidentes en diferentes categorías, pero en COBIT 2019 todos son incidentes.	**[433] No procede** Para las Superintendencias es relevante destacar el tema de la seguridad cibernética. 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 otra parte, se modifica la redacción para incluir referencia a seguridad de la información	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.
	[434]CAJAANDE Durante la gestión del incidente la prioridad es restaurar la operativa, se debe valorar hacer el análisis forense en una etapa posterior. Favor revisar redacción debido a que se presta para confusión, se refiere a recopilar las evidencias durante la gestión del incidente, y no al análisis forense como tal.	**[434] Procede** Se ajustó la redacción	
	[435]COOPENAE	**[435] Procede** Se ajustó la redacción	

	(Impacto Alto, Esfuerzo Medio) Define los criterios para gestionar un incidente, es detallado y obliga a las organizaciones a ser más diligentes en su gestión de incidentes.		
	[436]CCPA 1-Consideramos importante recalcar que este plan debe contener una sección de continuidad del negocio en caso de un ataque cibernético como los vividos en el país en el último periodo. 2-Además, agregar en el segundo párrafo que el análisis forense mencionado se realizara por profesionales autorizados como los Contadores Públicos Autorizados, que por su fe pública realizan este tipo de trabajos.	**[436] Procede** 1-Se ajustan las fases de los lineamientos generales del reglamento considerando parte de lo indicado en la observación. 2-No obstante, en relación con el punto 2, se determina que las entidades y empresas supervisadas pueden contratar proveedores a nivel internacional que brinden estos servicios y no proveedores en el mercado local.	
			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.
El proceso de gestión de incidentes debe establecer un plan de respuesta a incidentes de seguridad cibernética y los controles a fin de recopilar las evidencias para el análisis forense durante la gestión del incidente.	**[437]JUPEMA** ¿A qué se refiere con análisis forense? ¿Solo aplica para incidentes de SC no para incidentes de SI?	**[437]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.	~~El proceso de~~ La gestión de incidentes debe establecer un plan de respuesta a incidentes de seguridad de la información y seguridad cibernética ~~y~~, así como los controles ~~a fin de~~ que permitan recopilar las evidencias para el análisis forense ~~durante la gestión del incidente~~.
	[438]FEDEAC ¿Solo aplica para incidentes de Seguridad Cibernética no para	**[438] Procede** Se ajustó la redacción para incluir incidentes de seguridad de la información.	

	incidentes de Seguridad de Información?		
Artículo 37. Función de respuesta a incidentes de seguridad cibernética		Se modifica la redacción para incluir referencia a seguridad de la información	**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 cibernética, de conformidad con su estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados.	**[439]Luis Diego León Barquero** El marco de Gobierno y gestión de TI de COBIT 2019 tiene un objetivo de Gestionar Problemas, pero no hace distinción entre incidentes de seguridad de la información e incidentes de seguridad cibernética. De acuerdo con COBIT 2019, todos los problemas deben ser tratados de la misma manera. Puede ser necesario clasificar los problemas en diferentes categorías, pero en COBIT 2019 todos son Gestionar Problemas.	**[439]No procede** Para las Superintendencias es relevante destacar el tema de la seguridad cibernética. 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.	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.
	[440]JUPEMA ¿Solo aplica para incidentes de SC no para incidentes de SI?	**[440] Procede** Se ajustó la redacción para incluir incidentes de seguridad de la información.	
	[441]OPC-CCSS A lo largo del RGGTI se mencionan las nuevas responsabilidades en cuanto a la gestión de incidentes de seguridad cibernética, lo cual implicará costos en recurso humano, tecnología y tiempo para su cumplimiento. ¿Qué sucede con las empresas que operan al costo, se podrá implementar esto de forma gradual?	**[441]No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias	
	[442]BCR Respecto a la función de respuesta a incidentes, se definen responsabilidades puntales dentro del reglamento. ¿Esta figura se	**[442] No procede** La entidad, de conformidad con su modelo de negocio es la que establece quién ejecuta la función indicada en la disposición.	

	refiere a un comité o una unidad formal?		
	[443]CCPA De igual manera que el anterior comentario al artículo 36, es recomendable agregar términos para la continuidad del negocio en caso de un ataque.	**[443] Procede** Se ajustaron las fases de los lineamientos generales del reglamento considerando parte de lo señalado en la observación.	
La función de respuesta a incidentes de seguridad cibernética puede estar conformada por personal de diferentes áreas de la entidad o empresa supervisada, o cualquier otro miembro que se considere necesario.		Se modifica la redacción para incluir referencia a seguridad de la información	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 cibernética serán, al menos, las siguientes:		Se modifica la redacción para incluir referencia a seguridad de la información	Las principales actividades de la función de respuesta a incidentes de seguridad de la información y 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.			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.	**[444]CFBNCR** En el punto d) se sugiere ajustar el texto subrayado, donde considere erradicar o resolver el incidente: d) Detectar y prever acontecimientos y pasos a seguir en función del desarrollo de los hechos, para erradicar y resolver el incidente.	**[444] Procede** Se ajusta la disposición considerando parte de los comentarios.	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 e implementar estrategias de mejora continua.		Se modifica la redacción para incluir referencia a seguridad de la información y seguridad cibernética	e)Identificar oportunidades de mejora para la gestión de incidentes de seguridad de la información y seguridad cibernética, así como ~~e~~ implementar estrategias de mejora continua.
Artículo 38. Clasificación, registro y priorización de los incidentes de seguridad cibernética			**Artículo 38. Clasificación, registro ~~y priorización~~ e impacto de los incidentes de seguridad de la información y seguridad cibernética**

Las entidades y empresas supervisadas deben clasificar, registrar y priorizar los incidentes de seguridad cibernética, de conformidad con el esquema de clasificación y las categorías de impacto que están establecidos en los lineamientos generales del presente reglamento.	**[445]Luis Diego León Barquero** En este párrafo, considero que se debe cambiar las palabras de seguridad cibernética por seguridad de la información.	**[445] No procede** Para las Superintendencias es relevante destacar el tema de la seguridad cibernética. 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 otra parte, se ajustó la redacción para incluir tanto incidentes de seguridad de la información como de seguridad cibernética.	Las entidades y empresas supervisadas deben clasificar~~,~~ y registrar ~~y priorizar~~ los incidentes de seguridad de la información y seguridad cibernética, de conformidad con ~~el esquema de~~ la clasificación de incidentes y ~~las categorías~~ de su impacto~~, que están~~ establecidos en los lineamientos generales del presente reglamento.
	[446]JUPEMA ¿Solo aplica para incidentes de SC no para incidentes de SI?	**[446]No procede** Se modificó la redacción y se adicionaron los incidentes de seguridad de la información.	
	[447]COOPENAE (Impacto Alto, Esfuerzo Medio) Define los criterios para gestionar un incidente, es detallado y obliga a las organizaciones a ser más diligentes en su gestión de incidentes.	**[447] No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	
	[448]ISACA Es reiterada la observación de dejar fuera de lo explícito a la seguridad legal, administrativa y física.	**[448] No procede** La gestión de riesgos debe de realizarse de forma integral en la organización por 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.	
Artículo 39. Informes de comunicados de incidentes de seguridad cibernética a las Superintendencias		Se modifica la redacción para incluir referencia a seguridad de la información	**Artículo 39. ~~Informes de comunicados~~ Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias**
Las entidades y empresas supervisadas deben remitir a las respectivas Superintendencias, informes de	**[449]Luis Diego León Barquero**	**[449] No procede**	Las entidades y empresas supervisadas deben remitir a las respectivas Superintendencias, informes de

comunicados de los incidentes de seguridad cibernética cuando:	En este párrafo, considero que se debe cambiar las palabras de seguridad cibernética por seguridad de la información.	Se ajustó la redacción para incluir tanto incidentes de seguridad de la información como de seguridad cibernética. 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.	comunicados de los incidentes de seguridad de la información y seguridad cibernética cuando su impacto sea clasificado como "moderado" o "alto".~~:~~
	[450]MUCAP Existe la incertidumbre sobre el uso que le van a dar las superintendencias, a las bases de datos de los incidentes, siendo de importancia relevante que se pudiera compartir esa información, de forma agregada (sin nombre de entidades), lo que permite a las entidades tener un panorama de lo que está sucediendo en el entorno nacional.	**[450] No procede** En caso de que se detecten situaciones que puedan generar un contagio sistémico, se alertará sobre dicha situación. 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.	
	[451]JUPEMA Pregunta ¿Quién es el responsable de emitirlo?	**[451] Se atiende como consulta** La entidad o empresa supervisada debe establecerlo de conformidad con su modelo de negocio, tamaño y complejidad.	
	[452]COOPEMEP Se solicita la explicación en relación al contenido de los Informes sobre los Incidentes que puede no tenerse al momento de su remisión o puede variar el contenido al transcurrir el tiempo. Considerar que en muchas ocasiones el contenido relacionado a los Vectores de ataque no es posible determinarlo dentro de las primeras 8 horas sucedido el incidente, sin embargo, se solicita como	**[452] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos.	

	contenido en el Informe inicial de incidentes. Tampoco necesariamente se conoce a ciencia cierta dentro del plazo para enviar el Informe de avance de atención de incidentes, por lo cual se necesita comprender si se permite remitir el informe indicando que no se conoce la respuesta a este contenido, y podría darse que podría "cambiar" en el momento de una investigación forense, se permite modificar la respuesta a este contenido.		
	[453]FEDEAC Los plazos deberían considerar el tipo de evento e implicaciones de resolución, las áreas operativas estarán enfocadas en la resolución del incidente. Se ha considerado que el tamaño de algunos de departamentos de seguridad no es tan grande y que probablemente los responsables de atender los incidentes se encontrarán trabajando en detener o recuperar urgentemente a la entidad, entonces asignar tiempo para su atención podría significar una demora en la gestión pura del evento. La prioridad debe ser la atención de los incidentes y no los informes. Se solicita explicación en relación con el contenido de los Informes sobre los Incidentes que puede no tenerse al momento de su remisión o puede variar el contenido al transcurrir el tiempo. Considerar que en muchas ocasiones el contenido	**[453] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos.	

	relacionado a los Vectores de ataque no es posible determinarlo dentro de las primeras 8 horas de sucedido el incidente, sin embargo, se solicita como contenido en el Informe inicial de incidentes. Tampoco necesariamente se conoce a ciencia cierta dentro del plazo para enviar el Informe de avance de atención de incidentes, por lo cual se necesita comprender si se permite remitir el informe indicando que no se conoce la respuesta a este contenido, y podría darse que podría "cambiar" en el momento de una investigación forense, se permite modificar la respuesta a este contenido.		
	[454]COOPEBANPO Respecto al contenido de los Informes sobre los Incidentes, es posible que el toda la información que debe reportarse no se tenga disponible al momento de su remisión o puede variar el contenido al transcurrir el tiempo. Considerar que en muchas ocasiones el contenido relacionado a los Vectores de ataque no es posible determinarlo dentro de las primeras 8 horas sucedido el incidente, sin embargo, se solicita como contenido en el Informe inicial de incidentes. Tampoco necesariamente se conoce a ciencia cierta dentro del plazo para enviar el Informe de avance de atención de incidentes, por lo cual	**[454] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos.	

	se necesita comprender si se permite remitir el informe indicando que no se conoce la respuesta a este contenido, y podría darse que podría "cambiar" en el momento de una investigación forense, se permite modificar la respuesta a este contenido.		
	[455]AAP Se propone:1. Realizar una notificación Inicial del Incidente eliminando según lineamientos (cronograma, vectores de ataque, clasificación del incidente y descripción del Impacto) valorar el plazo inicial a mínimo 2 días.2. Eliminar el Informe de avance de atención de Incidente.3. Enviar el Informe post actividad una vez cerrado el Incidente. Adicional el canal de comunicación aclarar que el Hecho relevante debe ser privado. Lo anterior debido a que se considera que el plazo definido para realizar el informe no es adecuado ya que en la fase de Detección y análisis se está en proceso de identificar el origen del incidente, por esto no es adecuado utilizar tiempo para redactar el informe en vez de tener la afectación presentada. El informe se debería enviar una vez concluido el análisis del incidente. • El contenido del informe inicial, difícilmente se pueda tener todo el detalle solicitado porque las primeras horas son cruciales para detener el ataque e indagar los rastros para determinar el origen	**[455] No procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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.	

	de este.• Ampliar si el contenido inicial de los reportes puede variar según los acontecimientos. Los informes deben ser elaborados por personal de TI y los esfuerzos van a estar enfocados en la contención del ataque y el restablecimiento de los servicios para la continuidad del negocio. Ver sugerencias para la gestión de informes de incidentes. Por la complejidad técnica que necesita un comunicado masivo a clientes, considerar ampliar el plazo entre 5 y 10 días hábiles.		
	[456]CFBNCR Se sugiere la valoración de un ajuste en la redacción, ya que durante la fase de "detección y análisis" no se tiene certeza absoluta de que se trate de un incidente y se podría producir una falsa alarma innecesaria. 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 agradece 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,	**[456] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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 agradece su consideración al respecto.		
	[457]ABC Durante la fase de "detección y análisis" no se tiene certeza absoluta de que se trate de un incidente y se podría producir una falsa alarma innecesaria. 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. En virtud de lo anterior, se solicita modificar la norma para ajustar el momento del reporte a la lógica descrita en el párrafo anterior.	**[457] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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.	
	[458]CB Segundo párrafo: Comentarios: Se sugiere la valoración de un ajuste en la redacción, ya que durante la fase de "detección y análisis" no se tiene certeza absoluta de que se trate de un incidente y se podría producir una falsa alarma innecesaria. 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.	**[458] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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.	

	En abono a lo indicado, debemos señalar que el mismo Regulador ha experimentado incidentes que no le es posible explicar a los supervisados en esas fases, por su misma naturaleza. De tal forma que este no es un tema menor, sino que se plantea con base en la práctica y la realidad en esta materia, por lo que se solicita su consideración y valoración respectiva. Adicionalmente, sobre este mismo tema, en los Lineamientos Generales (Sección VIII de los Lineamientos) el Plazo que se establece para reportar el incidente (8 horas, según Sección VIII.1.ii de los Lineamientos) es demasiado corto y no es consistente ni con los estándares internacionales, ni con la compleja realidad de la atención de un incidente de ciberseguridad. Según los Lineamientos (sección VIII), el reporte inicial debe contener, entre otras cosas, una descripción general del incidente, vectores de ataque, clasificación del incidente, y descripción del impacto según las categorías establecidas en los Lineamientos. Sin embargo, esa información es prácticamente imposible de recolectar en 8 horas. Debe tomarse en cuenta que la identificación del origen, causa y dimensión de un incidente no es inmediatamente detectable, por lo que mantener este requisito de notificar en un plazo de 8 horas podría ser de imposible		

	cumplimiento. Se recomienda incrementar a 5 días hábiles, a partir de la identificación de que se trata de un incidente notificable. Último párrafo: Comentarios Sobre esta disposición se solicita aclarar sobre el objetivo y uso que le van a dar las superintendencias, a las bases de datos de los incidentes.		
	[459]SEGUROSLAFISE Se propone:1. Realizar una notificación Inicial del Incidente eliminando según lineamientos (cronograma, vectores de ataque, clasificación del incidente y descripción del Impacto) valorar el plazo inicial a mínimo 2 días. 2. Eliminar el Informe de avance de atención de Incidente.3. Enviar el Informe post actividad una vez cerrado el Incidente. Adicional el canal de comunicación aclarar que el Hecho relevante debe ser privado. Lo anterior debido a que se considera que el plazo definido para realizar el informe no es adecuado ya que en la fase de Detección y análisis se está en proceso de identificar el origen del incidente, por esto no es adecuado utilizar tiempo para redactar el informe en vez de tener la afectación presentada. El informe se debería enviar una vez concluido el análisis del incidente. • El contenido del informe inicial, difícilmente se pueda tener todo el detalle solicitado porque las primeras horas son cruciales para detener el ataque e indagar los	**[459] No procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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.	

	rastros para determinar el origen de este. • Ampliar si el contenido inicial de los reportes puede variar según los acontecimientos. Los informes deben ser elaborados por personal de TI y los esfuerzos van a estar enfocados en la contención del ataque y el restablecimiento de los servicios para la continuidad del negocio.		
	[460]COOPENAE (Impacto Alto, Esfuerzo Medio) Se hace relevante asegurar que se tiene un proceso preciso para identificación y gestión de los incidentes. Al requerir reportes históricos o de gestión, es claro que esta no puede ser desarrollada en herramientas como Excel. Por otra parte, el nivel de explicación del incidente es detallado, por lo que se debe considerar una función específica que se oriente a esta gestión.	**[460] 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, adicionalmente, se realizan ajustes a los lineamientos para aclarar el tema de las salvedades.	
	[461]CIS Se agradece y solicita la explicación en relación al contenido de los Informes sobre los Incidentes que puede no tenerse al momento de su remisión o puede variar el contenido al transcurrir el tiempo. Considerar que en muchas ocasiones el contenido relacionado a los Vectores de ataque no es posible determinarlo dentro de las primeras 8 horas sucedido el incidente, sin embargo, se solicita como contenido en el Informe inicial de incidentes. Tampoco	**[461] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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.	

	necesariamente se conoce a ciencia cierta dentro del plazo para enviar el Informe de avance de atención de incidentes, por lo cual se necesita comprender si se permite remitir el informe indicando que no se conoce la respuesta a este contenido, y podría darse que podría "cambiar" en el momento de una investigación forense, se permite modificar la respuesta a este contenido.		
	[462]ISTMO Considerar que en la fase de Detección y Análisis es complejo brindar informes, la prioridad se centra en eso, no en estar redactando informes. Más bien debe ser un comunicado simple, bajo condiciones mínimas y posterior a Mitigado y Recuperado, entonces si cumplir con la entrega de los informes correspondientes.	**[462] Procede** Se modificó la redacción del artículo y se realizaron los ajustes para las salvedades en los lineamientos. 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.	
	[463]ISACA 1-Es reiterada la observación de dejar fuera de lo explícito a la seguridad legal, administrativa y física. 2-Es importante comprender el nivel de detalle de este informe, ya que en estas etapas puede que algunos detalles no sean del todo claros o concretos, además que podrían desenfocar la labor y efectividad de la gestión al tomar decisiones con información de carácter parcial con respecto al incidente. Generalmente es práctica de la industria que cuando	**[463] No procede** 1- 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. 2-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, adicionalmente, se realizan ajustes a los lineamientos para aclarar el tema de las salvedades.	

	se detecta y está atendiendo el incidente la comunicación es muy general y posterior al restablecimiento de los servicios se hacen actualizaciones y al finalizar un proceso de investigación de causas raíces cuando corresponda se termine de ampliar detalles finales de lo ocurrido, lo que se realizó en el momento para contener la situación y lo que se hará para que no vuelva a ocurrir y cómo esto retroalimenta al proceso de gestión de riesgos de la entidad.		
a) presenten un impacto funcional “alto”;			~~a) presenten un impacto funcional “alto”;~~
b) presenten un impacto a la información en “violación de la privacidad, violación de la propiedad exclusiva o pérdida de integridad”, o	**[464]BPDC** Los elementos del punto b deben estar definidos y alineados con la ley 8968 El punto c debe limitarse a lo crítico	**[464] No procede** Se eliminó el párrafo de la disposición.	~~b) presenten un impacto a la información en “violación de la privacidad, violación de la propiedad exclusiva o pérdida de integridad”, o~~
c)el impacto a la capacidad de recuperación sea “extendido” o “no recuperable”.	**[464]BPDC** El punto c debe limitarse a lo crítico	**[464] No procede** Se eliminó el párrafo de la disposición.	~~c)el impacto a la capacidad de recuperación sea “extendido” o “no recuperable”.~~
Los informes de comunicados de incidentes de seguridad cibernética deben ser remitidos durante la fase de “Detección y análisis” y la fase de “Contención, mitigación y recuperación”, según corresponda.			Las Superintendencias podrán solicitar ~~Los~~ informes ~~de comunicados~~ sobre la atención de los incidentes de seguridad de la información o de seguridad cibernética ~~deben ser remitidos durante la fase de “Detección y análisis” y la fase de “Contención, mitigación y recuperación”, según corresponda~~.
Los tipos de informes de comunicados de incidentes de seguridad cibernética, los plazos y los formatos para su remisión están establecidos en los lineamientos generales del presente reglamento.			Los tipos de informes ~~de comunicados~~ 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 comunicarán, mediante acto administrativo, los canales de remisión de los informes de comunicados de los incidentes de seguridad cibernética.			Las Superintendencias informarán ~~comunicarán, mediante acto administrativo,~~ los canales de remisión de los comunicados y de los informes de ~~comunicados de los~~ 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 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.	**[465]Luis Diego León Barquero** En este párrafo, considero que se debe cambiar las palabras de seguridad cibernética por seguridad de la información.	**[465] No procede** Se agregó en la disposición que trata tanto de incidentes de seguridad de la información como de incidentes de seguridad cibernética.	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.
	[466]BPDC Se considera que dos días no es viable, dados los protocolos internos de escalamiento, se recomienda 5 días	**[466] Procede** Se ajusta la redacción con lo sugerido en la observación.	
	[467]MUCAP Esta norma, pese a que está enfocada en un principio de transparencia con el cliente, su aplicación irrestricta causaría un problema mayor, que podría desembocar en una corrida con afectación en la liquidez de una entidad supervisada, por la forma tan drástica en que está redactada. Aclarar, la norma regula dos supuestos: i) el momento en que se detecta el incidente; y ii) el momento de "cierre" del incidente. No obstante, la norma no indica para el primer supuesto (momento de "detección") en qué plazo debe comunicarse a los clientes, como sí lo hace para el segundo supuesto "cierre", o si al momento de detección no media comunicación a éstos.	**[467] No procede** La disposición indica que 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. El tiempo de comunicado debe de realizarse de forma oportuna, según el incidente.	
	[468]COOPEANDE	**[468]No Procede**	

	Valorar ampliar el plazo máximo de respuesta a 3 días hábiles. Muchas veces no se conoce la causa raíz rápido, y casi todo el personal estará concentrado en la recuperación. Por otra parte, no queda claro cuándo comunicar a los clientes sobre el incidente y planes de acción, cuando se sufrió qué afectación, a los datos personales, financieros? Se deja a libre interpretación., y si esto fuera así, se debería cuidar la reputación de la organización.	Se ajusta la redacción con lo sugerido en la observación [466], cabe señalar que la disposición indica que: Cuando la confidencialidad o integridad de la información de los clientes sea afectada debido a un incidente de seguridad cibernética, las entidades y empresas supervisadas deberán comunicarles a estos sobre la afectación. Será responsabilidad de las entidades y empresas supervisadas definir el tipo, el alcance y el contenido mínimo de la comunicación, la cual, deberá ser oportuna, clara y con un alcance apropiado en función del incidente.	
	[469]JUPEMA ¿Quién es el responsable de emitirlo?	**[469]No procede** Se atiende como consulta. La entidad conforme el articulo 34 debe establecer las unidades, funciones organizacionales, centros de operaciones y comentes técnicos, adicionalmente, el artículo 8 establece como responsabilidades del Órgano de Dirección la aprobación de dichas estructuras.	
	[470]FEDEAC 1-Valorar ampliar el plazo máximo de respuesta a 3 días hábiles. Muchas veces no se conoce la causa raíz rápido, y casi todo el personal estará concentrado en la recuperación. 2-¿Por otra parte, no queda claro cuándo comunicar a los clientes sobre el incidente y planes de acción, cuando se sufrió qué afectación, a los datos personales, financieros? Se deja a libre interpretación, y si esto fuera así, se debería cuidar la reputación de la organización.	**[470]No Procede** 1-Se ajusta la redacción con lo sugerido en la observación [466] 2-La entidad debe comunicar de manera oportuna los incidentes a sus clientes eso implica un tiempo prudencial definido por la entidad a través de sus políticas. 3-La profundidad de la afectación señala hace referencia a que se deben comunicar cuando la confidencialidad o integridad de la información de los clientes sea afectada debido a un incidente de seguridad cibernética,	

	3-¿No consideran el plazo o profundidad de afectación? (alto - medio) algunos incidentes pueden no ser significativos para ser comunicados. El plazo de notificación al cliente dependerá del diagnóstico correcto de la afectación.		
	[471]COOPESERVIDORES Aclarar si estos incidentes se extraen de las bases de eventos que se remiten en cumplimiento SGF 02-10 y, se reportarán de manera separada.	**[471] No procede** Las entidades y empresas supervisadas son las que establecen de conformidad con su tamaño, complejidad y modelo de negocio cómo realizar la gestión de los incidentes y dónde mantener los registros de los incidentes. Por otra parte, la disposición hace referencia al comunicado de incidentes que se debe realizar a los clientes y no a las superintendencias.	
	[472]CAJAANDE Cuando nos referimos a los 3 pilares de la Seguridad de la Información, este artículo no hace referencia al pilar de disponibilidad; ¿esto no necesariamente aplica y queda a criterio de las instituciones su tratamiento ante estos escenarios?	**[472] No procede** La disposición hace referencia a que el comunicado se realiza cuando la confidencialidad o integridad de la información de los clientes sea afectada debido a un incidente de seguridad cibernética, la disponibilidad no está incluida en esta disposición ya que esta se atiende en disposiciones relacionadas con la continuidad y la resiliencia cibernética.	
	[473]COOPEALIANZA Se solicita la siguiente redacción en el punto especifico: “Las medidas adoptadas para remediar el incidente se deben comunicar a los clientes en un plazo máximo de tres días hábiles posteriores al cierre del incidente.”	**[473]No Procede** Se ajusta la redacción con lo sugerido en la observación [466]	
	[474]VIDAPLENA 1-No queda claro si son dos o más comunicaciones o solo una	**[474]No Procede** La disposición indica que será responsabilidad de las entidades y	

	posterior a la remediación del incidente. 2-Habría que valorar impactos legales, de imagen, etc. En caso de suceder.	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. La cantidad de comunidad está en función de la forma oportuna. 2-Los incidentes relacionados a seguridad cibernética tienen ya impactos al exponer la confidencialidad o integridad de la información de los clientes y de las organizaciones, los cuales deben ser evaluados por las entidades y empresas supervisadas como parte de su gestión integral de riesgos.	
	[475]CB Se considera que dos días no es viable, dados los protocolos internos de escalamiento, se sugieren 5 días.	**[475]No Procede** Se ajusta la redacción con lo sugerido en la observación [466]	
	[476]SEGUROSLAFISE Por la complejidad técnica que necesita un comunicado masivo a clientes, considerar ampliar el plazo entre 5 y 10 días hábiles.	**[476] Procede** Se ajusta la redacción para indicar que son cinco días.	
	[477]BCR Pregunta • Incluir el elemento de Privacidad. • ¿Han analizado los impactos en el riesgo reputacional de las entidades en la atención de este artículo? Comunicado de incidentes a los clientes que sin duda es una buena práctica, ¿pero se debe de aplicar para qué casos o condiciones o impactos?	**[477]No procede** Se atiende como consulta. Los incidentes relacionados a seguridad cibernética tienen ya impactos relacionados al exponer la confidencialidad o integridad de la información de los clientes y de las organizaciones, los cuales deben ser evaluados por las entidades y empresas supervisadas como parte de su gestión integral de riesgos. Adicionalmente, en los lineamientos se incluyen disposiciones para las valoraciones de los impactos.	

Las medidas adoptadas para remediar el incidente se deben comunicar a los clientes en un plazo máximo de dos días hábiles posteriores al cierre del incidente.		Se ajusta la redacción con lo sugerido en la observación [466]	Además, las medidas adoptadas para remediar el incidente se deben comunicar a los clientes en un plazo máximo de ~~dos~~ cinco días hábiles posteriores al cierre del incidente.
Artículo 41. Reporte histórico de incidentes			**Artículo 41. Reporte histórico de incidentes de seguridad de la información y seguridad cibernética**
Las entidades y empresas supervisadas deben remitir a las respectivas Superintendencias un reporte histórico de los incidentes de seguridad cibernética cerrados que tuvieron un impacto funcional de sus sistemas de TI "medio" y "alto", los cuales presenten un impacto de "pérdida de integridad" de la información o que el impacto a la capacidad de recuperación sea "complementado", "extendido" o "no recuperable".	**[478]Luis Diego León Barquero** En este párrafo, considero que se debe cambiar las palabras de seguridad cibernética por seguridad de la información.	**[478] No procede** Se ajustó la redacción para incluir tanto incidentes de seguridad de la información como de seguridad cibernética. Se modifica la redacción del artículo y se elimina lo referente a que las entidades deban remitir el reporte histórico de incidentes.	Las entidades y empresas supervisadas deben elaborar ~~remitir a las respectivas Superintendencias~~ un reporte histórico de los incidentes de seguridad de la información y seguridad cibernética ~~cerrados que tuvieron un impacto funcional de sus sistemas de TI "medio" y "alto", los cuales presenten un impacto de "pérdida de integridad" de la información o que el impacto a la capacidad de recuperación sea "complementado", "extendido" o "no recuperable".~~ Dicho reporte deberá estar a disposición de las Superintendencias cuando estas lo requieran como parte de las labores de supervisión.
	[479]JUPEMA Pregunta ¿Quién es el responsable de emitirlo?	**[479]No procede** Se atiende como consulta. La entidad conforme el articulo 34 debe establecer las unidades, funciones organizacionales, centros de operaciones y comentes técnicos, adicionalmente el artículo 8 establece como responsabilidades del órgano de dirección la aprobación de dichas estructuras.	
	[480]CATHAY Es conveniente definir qué se entiende por un incidente de seguridad cibernética y el alcance que este tiene en cuanto al reporte a la Superintendencia. Es decir, si este incluye ataques cibernéticos efectuados a clientes o si por el contrario solo aquellos que tienen una incidencia directa para la organización.	**[480] No procede** El Artículo 36. Gestión de incidentes de seguridad cibernética, dispone que las entidades y empresas supervisadas deben asegurar que el diseño e implementación de la gestión de incidentes de la organización incorpore las fases establecidas en los lineamientos generales del presente reglamento para la gestión de incidentes de seguridad cibernética.	

		Por otra parte, en la propuesta de modificación reglamentaria se establece que, 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.	
	[481]AAP Favor aclarar la recurrencia de esa potencial petición de Sugese, porque esto implica cargas operativas. Debido a los potenciales problemas reputacionales que el acceso público puede traer, Favor considerar cambiar el canal de comunicación a canales privados como XML u otro similar.	**[481] No procede** Se ajustó la redacción para aclarar que dicho reporte deberá estar a disposición de las Superintendencias cuando estas lo requieran como parte de las labores de supervisión.	
	[482]CAJAANDE Favor ampliar como se podría generar este dato de impacto funcional, ¿se podría generar basado en las pérdidas económicas?	**[482] No procede** La clasificación de los impactos está definida en los lineamientos generales de la propuesta de modificación reglamentaria. Adicionalmente se eliminó lo referente a impacto funcional.	
	[483]SMSEGUROS Por favor considerar un medio privado para la entrega de la información de los sujetos obligados de SUGESE, ya que los hechos relevantes de SUGESE son de carácter público.	**[483] No procede** El medio definido contiene pautas para salvaguardar el contenido del comunicado, por lo que, la Superintendencia lo considera adecuado, 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.	
	[484]SEGUROSLAFISE	**[484] No procede**	

	Favor aclarar la recurrencia de esa potencial petición de Sugese, porque esto implica cargas operativas. Debido a los potenciales problemas reputacionales que el acceso público puede traer, Favor considerar cambiar el canal de comunicación a canales privados como XML u otro similar.	Se ajustó la redacción para aclarar que dicho reporte deberá estar a disposición de las Superintendencias cuando estas lo requieran como parte de las labores de supervisión.	
	[485]COOPENAE Consideramos clave tener los alcances claros sobre los tipos de reportes a generar, su periodicidad, el alcance, si involucra temas de fraude o solo se circunscribe temas propios de hackeo, pues la norma propuesta es muy general en esta línea. Por lo cual consideramos importante en la normativa definir claramente estos aspectos y no dejar luego a interpretaciones de cada regulador o de cada institución ese tipo de requerimientos de información.	**[485] No procede** El contenido del reporte histórico de incidentes está establecido en los lineamientos generales del reglamento.	
	[486]CIS Se sugiere la eliminación para los supervisados por SUGESE, que el canal de remisión sea como Hecho relevante, siendo que esto es de acceso público lo cual podría no ser conveniente (Sección IX. Lineamientos relacionados con el contenido, canales, plazos y el transitorio para la remisión del reporte histórico de los incidentes de seguridad cibernética) y elegir otro canal diferente.	**[486]No procede** El medio definido contiene pautas para salvaguardar el contenido del comunicado, por lo que, la Superintendencia lo considera adecuado, 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.	
	[487]ISTMO No se indica tiempos o períodos de tiempo para los informes	**[487] No procede** Se aclara que no son informes, es un reporte histórico. Por otra parte, se	

	históricos, se habla de plazos de remisión. Importante aclarar este punto. Incorporar en el artículo 4, las definiciones sobre capacidades de recuperación, "completado", "extendido" o "no recuperable"	modificó la redacción y ahora se indica que: el reporte deberá estar a disposición de las Superintendencias cuando estas lo requieran como parte de las labores de supervisión. Asimismo, que las Superintendencias comunicarán los canales de remisión del reporte histórico de los incidentes de seguridad de la información y seguridad cibernética.	
	[488]ISACA Puede que esto esté especificado en el lineamiento pero la definición de medio y alto es importante para evitar diferencias de criterio en cuanto al cumplimiento.	**[488] No procede** Se eliminó lo referente a medio y alto.	
El contenido, los canales y los plazos de remisión del reporte están establecidos en los lineamientos generales del presente reglamento.			El contenido~~, los canales y los plazos de remisión~~ del reporte está~~n~~ establecido~~s~~ en los lineamientos generales del presente reglamento.
		Se modifica la redacción del artículo y se elimina lo referente a que las entidades deban remitir el reporte histórico de incidentes.	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.	**[489]COOPEFYL** Debe revisarse la aplicación de este artículo a la luz de lo que establece el artículo 3 del presente reglamento y lo definido en el anexo 2 de los lineamientos generales ya que están en contraposición.	**[489] No procede** Las disposiciones señalan que las entidades y empresas supervisadas sujetas a la aplicación del artículo 3 deben remitir el perfil tecnológico, y revelar en este los procesos de evaluación del marco de gobierno y gestión de TI, los cuales, deben estar en consonancia con los indicados en el anexo 2.	Las entidades y empresas supervisadas deben elaborar su perfil tecnológico y actualizarlo
	[490]BNCR ¿Dónde se pueden consultar las nuevas tablas de referencia de la clase de datos 24 Perfil	**[490]No procede** Se atiende como consulta.	

	Tecnológico, ¿dado que en el reglamento se habla de algunos campos relacionados a ciberseguridad?	Las superintendencias publicaran a través de sus sitios web los archivos correspondientes al perfil tecnológico.	
	[491]BAC Los cambios que se estarán solicitando al perfil tecnológico posteriormente, que no fueron incluidos en los lineamientos generales, sino que se enviarán por oficio, ¿Pueden tener una prórroga para ser enviados en el perfil tecnológico del 2025? Esto para poder realizar todos los ajustes en las estructuras durante el 2024 pero sin afectar la entrega de este año.	**[491]Procede** Se incluyen disposiciones transitorias para la remisión del perfil de TI	
	[492]ABC El Reglamento no especifica el plazo para implementar los cambios, dado que lo dispuesto en la norma implica modificar las estructuras de SIVECA para remitir la información.	**[492]Procede** Se incluyen disposiciones transitorias para la remisión del perfil de TI	
	[493]ISACA 1-El establecer plazos y canales de remisión del perfil tecnológico está excelente, pero el contenido del mismo debe ser revisado, no se requiere tanta información en ese momento, mucha de la información debe ser recaba durante la auditoría externa o bien debe ser cotejada a través de un calendario distribuido en el año. 2-El área de control interno de TI debe ser mandatorio, o a nivel empresarial, que deberá ser por lo menos un área unipersonal dedicado al 100% del tiempo al	**[493] No procede** 1-La propuesta de modificación reglamentaria contiene las expectativas que las Superintendencias esperan que las entidades y empresas supervisadas gestionen, considerando sus riesgos, tamaño, complejidad y modelo de negocio. 2-La entidad conforme el articulo 34 debe establecer las unidades, funciones organizacionales, centros de operaciones y comentes técnicos, adicionalmente el artículo 8 establece como responsabilidades del órgano de dirección la aprobación de dichas estructuras.	

	cumplimiento de este reglamento y de las normativas internas y externas relacionadas.		
En los casos en que se cuente con una gestión de TI corporativa, un Comité de TI corporativo o sus respectivas funciones equivalentes a nivel corporativo, el grupo o conglomerado financiero podrá remitir un único perfil tecnológico al supervisor responsable.			En los casos en que se cuente con una gestión de TI corporativa, un Comité de TI corporativo o sus respectivas funciones equivalentes a nivel corporativo, el grupo o conglomerado financiero podrá remitir un único perfil tecnológico al supervisor responsable.
En cualquier caso, el perfil debe ajustarse al marco de gobierno y de gestión de TI de las entidades y empresas supervisadas que conforman el grupo o conglomerado e identificará las particularidades de cada una de estas.			En cualquier caso, el perfil debe ajustarse al marco de gobierno y de gestión de TI de las entidades y empresas supervisadas que conforman el grupo o conglomerado e identificará las particularidades de cada una de estas.
El contenido del perfil tecnológico y la guía para la descarga, llenado y remisión vigentes se encuentran en los sitios electrónicos oficiales de cada Superintendencia. Los plazos y los canales de remisión del perfil tecnológico están establecidos en los lineamientos generales del presente reglamento.		Se modifica la redacción del artículo para hacer referencia a que la información citada está en los lineamientos generales del reglamento.	~~El contenido del perfil tecnológico y la guía para la descarga, llenado y remisión vigentes se encuentran en los sitios electrónicos oficiales de cada Superintendencia.~~ 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 ~~están establecidos en los lineamientos generales del presente reglamento~~.
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.	**[494]COOPEFYL** Debe revisarse la aplicación de este artículo a la luz de lo que establece el artículo 3 del presente reglamento y lo definido en el anexo 2 de los lineamientos generales ya que están en contraposición.	**[494] No procede** Las disposiciones señalan que las entidades y empresas supervisadas sujetas a la aplicación del artículo 3 deben remitir el perfil tecnológico, y revelar en este los procesos de evaluación del marco de gobierno y gestión de TI, los cuales, deben estar en consonancia con los indicados en el anexo 2.	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.
	[495]COOPEANDE Es importante considerar que la Entidad tenga que reportar en el caso de los procesos que apliquen en el alcance del Marco de Gobierno y Gestión de TI, hasta que nivel de capacidad se	**[495] No procede** La entidad debe revelar los procesos aplicables. Las superintendencias no requieren que las entidades diseñen o implemente un nivel de capacidad o nivel de madurez especifico.	

	implementaran con el fin de generar valor a la estrategia y tener un balance adecuado costo-beneficio.	Para la implementación de las brechas del presente reglamento, se incluye la disposición transitoria respectiva.	
	[496]COOPEMEP Se solicita la explicación del periodo que tendrán las organizaciones para que los estudios técnicos sean desarrollados, entregados a los Supervisores y aceptados siendo que* las organizaciones deben identificar cuáles procesos le resultan adecuados a su marco de gobierno y gestión de TI de los 34 posibles ahora a 40 posibles, así como fundamentar aquellos que no les apliquen Se solicita la explicación en referencia a los Lineamientos para el Estudio Técnico, cómo interpretar el contenido exigido de analizar los Factores de diseño adaptados a la entidad o empresa supervisada? se puede modificar el abordaje establecido para el diseño del Marco de Gestión de TI por Cobit 2019 a otro enfoque distinto? o será exigido seguir literalmente esos factores de diseño?	**[496] No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	
	[497]FEDEAC Es importante considerar que la Entidad tenga que reportar en el caso de los procesos que apliquen en el alcance del Marco de Gobierno y Gestión de TI, hasta qué nivel de capacidad se implementaran con el fin de generar valor a la estrategia y tener un balance adecuado costo-beneficio.	**[497] No procede** La entidad debe revelar los procesos aplicables. Las superintendencias no requieren que las entidades diseñen o implementen un nivel de capacidad o nivel de madurez especifico. Para la implementación de las brechas del presente reglamento, se incluye la disposición transitoria respectiva.	

	[498]COOPEBANPO Solicitar la explicación del periodo que tendrán las organizaciones para que los estudios técnicos sean desarrollados, entregados a los Supervisores y aceptados siendo que* las organizaciones deben identificar cuáles procesos le resultan adecuados a su marco de gobierno y gestión de TI de los 34 posibles ahora a 40 posibles, así como fundamentar aquellos que no les apliquen* las organizaciones con regulación proporcional deben fundamentar cuáles procesos le resultan adecuados a su marco de gobierno y gestión de TI de los que actualmente lo componen a como mínimo los indicados en el Anexo 2 de los Lineamientos, así como fundamentar aquellos que no les apliquen no es claro, en referencia a los Lineamientos para el Estudio Técnico, ¿cómo interpretar el contenido exigido de analizar los Factores de diseño adaptados a la entidad o empresa supervisada? se puede modificar el abordaje establecido para el diseño del Marco de Gestión de TI por Cobit 2019 a otro enfoque distinto? o será exigido seguir literalmente esos factores de diseño?	**[498] No procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	
	[499]AAP Con respecto al tercer párrafo: Este párrafo lesiona el principio de proporcionalidad, habilitar a la Sugese con la potestad de que decida el marco de cada empresa, es un retroceso, es coadministrar.	**[499] No procede** En virtud de las facultades que el marco legal otorga al regulador, las Superintendencias podrán ampliar la cantidad de procesos de evaluación declarados en el perfil tecnológico de acuerdo con las necesidades de 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.	
	[500]VIDAPLENA 1-Considerando con lo anterior, es importante tomar en cuenta que la inclusión de un objetivo en el Marco de Gestión de la empresa requiere un plazo importante para su implementación; por lo tanto, esos temas se deberían considerar en este reglamento. 2-También sería importante que, el personal encargado de estos temas en las superintendencias tenga el nivel de un Auditor CISA, considerando que, si es un auditor CISA la persona indicada para realizar una auditoría de este nivel, igual conocimiento debería tener los trabajadores que revisan la información y dan su opinión en las Superintendencias. 3-Sobre lo indicado en el anexo 3; se debería mantener lo indicado en COBIT 2019; ubicarlo de 2 a 5, es importante recordar que, de acuerdo con el análisis de cada objetivo, así se define la capacidad requerida para la empresa; no podría decirse entonces, que lo requerido para tal o cual objetivo sea capacidad 2 y la firma auditora otorgándole una calificación de aceptable o fuerte, ya que la capacidad es conforme con lo requerido por la empresa. En este caso, COBIT2019 define del 2 al 5; incluso alguno de los objetivos	**[500] No procede** 1-Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias. 2- En relación con CISA, se considerará para posibles análisis de estructuras organizacionales. 3-Las Superintendencias no requieren que las entidades diseñen o implemente un nivel de capacidad o nivel de madurez especifico, adicionalmente se aclara en las respectivas secciones de preguntas y respuestas que se dispondrán en los sitios web de cada Superintendencias.	

	no tiene capacidad 2 o capacidad 5.		
	[501]ABC El alcance de la auditoría externa respecto de los proveedores de bienes y servicios de TI se debe limitar a los procesos específicos en los cuales están directamente involucrados con la entidad.	**[501] Procede** Se ajusta la redacción con parte de la observación del inciso e) del artículo 47 Alcance de la AE de TI.	
	[502]OPC-CCSS 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.	**[502] No procede** Las Superintendencias no requieren que las entidades diseñen o implemente un nivel de capacidad o nivel de madurez especifico, adicionalmente se aclara en las respectivas secciones de preguntas y respuestas que se dispondrán en los sitios web de cada Superintendencias.	
	[503]SEGUROSLAFISE Este párrafo lesiona el principio de proporcionalidad, habilitar a la Sugese con la potestad de que decida el marco de cada empresa, es un retroceso, es coadministrar.	**[503] No procede** En virtud de las facultades que el marco legal otorga al regulador, las Superintendencias podrán ampliar la cantidad de procesos de evaluación declarados en el perfil tecnológico de acuerdo con las necesidades de 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.	
	[504]CIS Se agradece y solicita la explicación del periodo que tendrán las organizaciones para	**[504 plazo] No procede** Para el cierre de las brechas que pueda tener la entidad en relación con las	

	que los estudios técnicos sean desarrollados, entregados a los Supervisores y aceptados siendo que* las organizaciones deben identificar cuáles procesos le resultan adecuados a su marco de gobierno y gestión de TI de los 34 posibles ahora a 40 posibles, así como fundamentar aquellos que no les apliquen* las organizaciones con regulación proporcional deben fundamentar cuáles procesos le resultan adecuados a su marco de gobierno y gestión de TI de los que actualmente lo componen a como mínimo los indicados en el Anexo 2 de los Lineamientos, así como fundamentar aquellos que no les apliquen Solicitar la explicación en referencia a los Lineamientos para el Estudio Técnico, cómo interpretar el contenido exigido de analizar los Factores de diseño adaptados a la entidad o empresa supervisada? se puede modificar el abordaje establecido para el diseño del Marco de Gestión de TI por Cobit 2019 a otro enfoque distinto? o será exigido seguir literalmente esos factores de diseño? Es decir, se agradece confirmar que se deberán implementar los 9 procesos indicados y que para los no aplicables, no será exigido el estudio técnico, por su complejidad, costos y el hecho de que no se cuenta con la información requerida para las variables por incorporar en la	disposiciones del presente reglamento, se incluyó un transitoriO. Para efectos de la evaluación de la gestión de TI, al menos se van a considerar 9 procesos, sin embargo, no se limitan a dichos procesos, cuando la entidad o empresas supervisada por su naturaleza, tamaño, y complejidad implemente más procesos para mantener un adecuado control interno en procura de salvaguardar sus activos de información.	

	evaluación, dado el incipiente estado de las cosas en las sociedades corredoras de seguros.		
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.
		Se agrega párrafo para mejorar el entendimiento de la disposición.	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, mediante acto administrativo, las Superintendencias podrán ampliar la cantidad de procesos de evaluación declarados en el perfil tecnológico de acuerdo con las necesidades de supervisión, el riesgo identificado o cuando se determine que el marco de gobierno y gestión de TI no es acorde con las particularidades de las entidades o empresas supervisadas.			Sin perjuicio de lo anterior, ~~mediante acto administrativo,~~ las Superintendencias podrán ampliar la cantidad de procesos de evaluación declarados en el perfil tecnológico de acuerdo con las necesidades de supervisión, el riesgo identificado o cuando se determine que el marco de gobierno y gestión de TI no es acorde con las particularidades de las entidades o empresas supervisadas.
Los criterios de calificación de los procesos de evaluación del marco de gobierno y gestión de TI están establecidos en el anexo 3 de los lineamientos generales del presente reglamento.	**[505]Luis Diego León Barquero** Los anexos no están en este documento.	**[505] No procede** La disposición indica que: 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.	**[506]Luis Diego León Barquero** El Anexo no está.	**[506] No procede** La disposición indica que: están establecidos en el anexo 3 de los lineamientos generales del presente reglamento.	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.
	[507]COOPEFYL Debe revisarse la aplicación de este artículo a la luz de lo que establece el artículo 3 del presente reglamento y lo definido en el	**[507] No procede** El artículo 3 indica que lo dispuesto en el Capítulo V La auditoría externa de TI, será de aplicación plena, salvo lo dispuesto en el artículo 43. Procesos de	

	anexo 2 de los lineamientos generales ya que están en contraposición.	evaluación del marco de gobierno y gestión de TI, en el artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética.	
	[508]AAP Favor aclarar el uso de las categorías de las funciones de la seguridad cibernética dentro del perfil tecnológico a nivel operativo. Proveer un ejemplo.	**[508] No procede** Los perfiles tecnológicos con las respectivas guías de cumplimentación serán publicados en cada uno de los sitios web de las superintendencias.	
	[509]SEGUROSLAFISE Favor aclarar el uso de las categorías de las funciones de la seguridad cibernética dentro del perfil tecnológico a nivel operativo. Proveer un ejemplo.	**[509] No procede** Los perfiles tecnológicos con las respectivas guías de cumplimentación serán publicados en cada uno de los sitios web de las superintendencias.	
	[510]ISACA Resulta dudoso el por qué se enfrascan en la gestión de riesgos de cibernética, de hecho, son los más fáciles de gestionar por tratarse de hardware y software, pero los riesgos de seguridad legal, seguridad administrativa, y seguridad física son de difícil gestión. Aunque los riesgos de cibernética estén gestionados adecuadamente, los eventos adversos sobre el tratamiento de la información en el ámbito legal, administrativo o físico podrían hacer que esa gestión cibernética no tenga mayor relevancia en el momento de acceso no autorizado o robo de información, dos eventos que no necesariamente están relacionados con la cibernética. Precisamente, se necesita una norma estandarizada por servicio	**[510] No procede** Para las Superintendencia es relevante definir disposiciones reglamentarias en relación con la seguridad cibernética. 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.	

	tecnológico financiero en función de la naturaleza de la entidad (cooperativas, financieras, bancos, corredurías, etc). En este caso se está analizado una norma para un mismo nicho de mercado segmentado en servicios tecnológicos financieros. Es funcional que se definan las categorías de una lista taxativa, pero los controles deben ser otorgados por el Fiscalizador.		
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**
Cuando se presenten cambios significativos en el perfil tecnológico con respecto al perfil anterior remitido a la Superintendencia, las entidades y empresas supervisadas deben comunicar dichos cambios.	**[511]COOPEFYL** Debe revisarse la aplicación de este artículo a la luz de lo que establece el artículo 3 del presente reglamento y lo definido en el anexo 2 de los lineamientos generales ya que están en contraposición.	**[511] No procede** El artículo 3 indica que lo dispuesto en el Capítulo V La auditoría externa de TI, será de aplicación plena, salvo lo dispuesto en el artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI, en el artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética.	~~Cuando se presenten~~ Las entidades y empresas supervisadas deben identificar los cambios ~~significativos~~ que se realicen en el perfil tecnológico con respecto al perfil anterior ~~remitido a la Superintendencia, las entidades y empresas supervisadas deben comunicar dichos cambios~~ , los cuales, consideren que son significativos. Lo anterior, en virtud de su naturaleza, tamaño, complejidad, modelo de negocio y riesgos.
	[512]COOPEBANPO Este articulo da la sensación de que, si durante el año, hay cambios significativos (no se sabe que es un cambio significativo) debe ser comunicado, sin embargo, en los lineamientos se establece que se hace en el mes que corresponde el	**[512] No procede** En los lineamientos se indica, entre otros aspectos, los plazos y canales para la remisión de los cambios significativos del perfil tecnológico.	

	envío, entonces, básicamente ¿el perfil se sigue enviando una vez al año y actualizarlo conforme a la práctica actual, con los cambios que se han presentado?		
	[513]CAJAANDE Ampliar a que nos referimos con cambios significativos.	**[513] Procede** Se modifica la redacción de la disposición para mejorar el entendimiento.	
	[514]BCR Por favor clarificar ¿Qué se considera como un cambio significativo en el Perfil Tecnológico?	**[514] Procede** Se modifica la redacción de la disposición para mejorar el entendimiento.	
	[515]ISTMO Definición de "cambio significativo en el perfil tecnológico", es relativo. Sugerencia: Dejar bien clara la definición.	**[515] Procede** Se modifica la redacción de la disposición para mejorar el entendimiento	
	[516]ISACA 1-Una cosa es un cambio significativo en una plataforma computacional y otra es un cambio significativo en el perfil tecnológico, ¿este segundo sería interpretado como un cambio de alcance? ¿Qué es un cambio significativo del perfil tecnológico? 2-De ser un cambio de alcance, la entidad o empresa supervisada debería ejecutar una nueva auditoría externa de TI, o en su defecto, si esta es reciente, entonces la auditoría deberá ser interna con participación de los principales interesados.	**[516] Procede** 1-Se modifica la redacción de la disposición para mejorar el entendimiento. 2-Por otra parte, lo señalado en el punto 2 no procede, ya que, los alcances de la Auditorías externas serán solicitados por las Superintendencias de conformidad con lo establecido en el artículo 47, y no están estrictamente relacionados con un cambio del perfil tecnológico.	
El plazo y los canales de comunicación de los cambios significativos del perfil tecnológico están establecidos en los lineamientos generales del presente reglamento.		Se modifica la redacción de lo dispuesto para mejorar el entendimiento según las observaciones.	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.	**[517]Luis Diego León Barquero** A pesar de la existencia del Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA, en Costa Rica, el Colegio de Contadores Públicos adoptó el Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Trabajos para Atestiguar y Servicios Relacionado de la Federación Internacional de Contadores (IFAC, por sus siglas en inglés). Este documento contiene las Normas Internacionales de Auditoría y Aseguramiento. El Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) versión 4 del 2020 tiene 106 páginas. El Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Trabajos para Atestiguar y Servicios Relacionado del IFAC cuenta con 1.243 páginas. Muchos dentro del campo de la auditoria, opinamos que las Normas Internacionales de Auditoría y Aseguramiento de la IFAC son más completas que el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF). Mi propuesta	**[517] No procede** Se adiciona texto para mejorar el entendimiento del artículo. La propuesta reglamentaria contiene las expectativas que las superintendencias esperan que los auditores externos de TI y las entidades y empresas supervisadas cumplan para la aplicación de los encargos de la 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.

	es cambiar utilizar las Normas Internacionales de Auditoría y Aseguramiento de la IFAC para la auditoría de sistemas.		
	[518]COOPEFYL Debe revisarse la aplicación de este artículo a la luz de lo que establece el artículo 3 del presente reglamento y lo definido en el anexo 2 de los lineamientos generales ya que están en contraposición.	**[518]No procede** El artículo 3 indica que lo dispuesto en el Capítulo V La auditoría externa de TI, será de aplicación plena, salvo lo dispuesto en el artículo 43. Procesos de evaluación del marco de gobierno y gestión de TI, en el artículo 44. Funciones para la evaluación de la gestión de riesgos de seguridad cibernética.	
	[519]MUCAP Analizar que puede resultar muy complicado para las entidades ejecutar esta auditoría en empresas transnacionales.	**[519] Procede** Se ajusta la redacción para aclarar las disposiciones considerando parte de lo señalado en la observación, indicando lo siguiente: "Cuando las entidades y empresas supervisadas dispongan de sus componentes tecnológicos mediante el uso de servicios de computación en la nube proveídos por terceros, las Superintendencias podrán valorar la aceptación de informes de auditorías externas con las que ya cuenten dichos proveedores. La auditoría externa de TI deberá ser realizada de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA, salvo en los casos en que se trate de proveedores de servicios de computación en la nube que ya cuentan con auditorías independientes".	
	[520]COOPEANDE Además, las Superintendencias, según los riesgos identificados, podrán solicitar a las entidades y empresas supervisadas la	**[520] Procede** Se ajusta la redacción para aclarar las disposiciones considerando parte de lo señalado en la observación	

	contratación de auditorías externas de TI para sus proveedores de bienes y servicios de TI. Valorar casos donde fabricantes de clase mundial no permitan recibir una auditoría puntual solicitada por la Entidad, para esto los fabricantes tienen evaluaciones y auditorías que hacen públicas y que cumplen con las buenas prácticas.		
	[521]JUPEMA ¿El alcance de las Auditoría Externa lo va a definir el ente regulador?	**[521]No procede** Se atiende como consulta. Según el Artículo 46. Auditoría externa de TI, el alcance es determinado por el supervisor.	
	[522]FEDEAC La Superintendencias podrán solicitar auditorías externas para los proveedores de la entidad supervisada, aspecto que debe considerarse en los contratos con los proveedores, sobre todo proveedores internacionales. 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. Valorar casos donde fabricantes de clase mundial no permitan recibir una auditoría puntual solicitada por la Entidad, para esto los fabricantes tienen evaluaciones y auditorías que hacen públicas y que cumplen con las buenas prácticas.	**[522] Procede** Se ajusta la redacción para aclarar las disposiciones considerando parte de lo señalado en la observación	
	[523]COOPEBANPO Hasta el día de hoy, cada vez que la sugef envía la solicitud de auditoría, se hace necesario aclarar	**[523] No procede** Las entidades y empresas supervisadas cuentan con un plazo no mayor de nueve meses para la contratación,	

	alcances, y NUNCA prorrogan el plazo que se tarda mientras hacen las aclaraciones, esto pone a las entidades en desventaja respecto al ente supervisor. (por ejemplo, a mí la última vez duraron más de un mesen darme la aclaración del alcance y durante este tiempo no pude hacer contratación. Deberían establecer dentro del plazo, un periodo prudencial de al menos 1 mes para hacer aclaraciones y después de ahí que cuente el plazo para la contratación, realización y entrega de los informes.	planificación, ejecución, revisión interna de los resultados, remisión de los productos de la auditoría externa de TI y solicitud de la presentación de los resultados finales de la auditoría externa de TI.	
	[524]CAMBOLSA Si bien es cierto se reconoce la importancia de la función de TI dentro del negocio y el papel crucial de los proveedores de servicios dentro de la dinámica de una empresa, la medida propuesta no incluye que tipo de parámetros va a utilizar la Superintendencia para hacer la solicitud, resulta importante que se establezca de en la normativa dicho parámetros a fin de brindar seguridad jurídica y que las entidades y empresas supervisadas sepan bajo que supuestos esto puede ser exigido y el alcance de la auditoria, con la experiencia actual la de la Auditoria de TI que establece el Reglamento vigente o recientes auditorias como las establecidas para el SINPE, sabemos que una auditoria en TI tiene una estimación mínima de $20,000, eso encarecía los gastos operativos de las entidades y empresa	**[524] No procede** El articulo 47 indica lo aspectos que se considerarán para definir el alcance de la auditoría externa de TI. 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.	

	supervisadas o incluso podría desincentivar la participación de empresas proveedoras en el mercado nacional al tener que someterse a auditorias por parte de terceros. Este tipo de medidas impositivas parecen ser un contrasentido al marco de gestión de TI que establece el Reglamento en consulta en el sentido, porque no es la empresa con base en su gestión de riesgo la que está determinando si es necesario una auditoria o no, sino la Superintendencia sin queda claro de antemano bajo que parámetros se va a solicitar Ante esta situación se considera importante que se valide la satisfacción de ese requisito a través de otro tipo de mecanismos tales como: 1- Informes de auditoría externos contratados por la empresa proveedora. 2- Si la empresa posee certificaciones adicionales, tal como ISO 27001, ISO 27002, ISO 27005, ISO 30001, NIST 800-30, o alguna relacionada con calidad, seguridad, u otro asociado. 3- A través de informes tipo declaraciones juradas del representante legal sobre la situación que requieran indagar.		
	[525]BCR 1-Complementar la responsabilidad del Comité de TI respecto a las calidades de los auditores externos.	**[525] No procede** 1-El reglamento indica en Artículo 13. Responsabilidades del Comité de TI o de la función equivalente en el inciso g) Validar que la firma de auditores externos o el profesional independiente	

	2-En contratos de suscripción no es posible solicitarle al proveedor una auditoría externa, a una empresa que no está sujeta a esta regulación.	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. 2- Se ajusta la redacción para aclarar las disposiciones con parte de los comentarios de la observación. 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.	
	[526]CIS Se considera relevante que el enfoque de SBR se refuerce en supervisores y en auditores externos, con el fin de que no se pretenda una implementación estandarizada con el resto de participantes del sector financiero, porque incluso ni en el mismo sector, las entidades son "estandarizables". Asimismo que se enfatice que la auditoría debe hacerse en función del nivel de riesgo asumido y no mediante la utilización de listas de verificación para una auditoría de mero cumplimiento sino más bien con un enfoque prospectivo y basada en riesgos.	**[526] No procede** Se modificó la matriz de evaluación de auditores externos a fin de mitigar aspectos como los indicados.	
	[527]CCPA Recomendamos adicionar el Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Trabajos para Atestiguar y	**[527] No procede** Además, lo siguiente: La auditoría externa de TI deberá ser realizada de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de	

	Servicios Relacionado adoptado por el Colegio, este documento contiene las Normas Internacionales de Auditoría y Aseguramiento, por ser una de las normativas internacionales más utilizada para los trabajos de auditoría o aseguramiento.	ISACA, salvo en los casos en que se trate de proveedores de servicios de computación en la nube que ya cuentan con auditorías independientes.	
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.	**[528]CB** Según lo comentado en disposiciones anteriores sobre la tercerización con empresas transnacionales, es importante señalar que puede resultar muy complicado para las entidades ejecutar esta auditoría en empresas transnacionales.	**[528] Procede** Se ajusta la redacción para aclarar las disposiciones con parte de los comentarios de la observación. 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.	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.
		Se incluye párrafo a fin de aclarar lo indicado en las observaciones del artículo 46.	Cuando las entidades y empresas supervisadas dispongan de sus componentes tecnológicos mediante el uso de servicios de computación en la nube proveídos por terceros, las Superintendencias podrán valorar la aceptación de informes de auditorías externas con las que ya cuenten dichos proveedores.
La auditoría externa de TI deberá ser realizada de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA.		Se incluye párrafo a fin de aclarar lo indicado en las observaciones del artículo 46.	La auditoría externa de TI deberá ser realizada de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA, salvo en los casos en que se trate de proveedores de servicios de computación en la nube que ya cuentan con auditorías independientes.
Las entidades y empresas supervisadas deben cumplir con lo dispuesto en el Reglamento General de Auditores Externos, Acuerdo CONASSIF 1-10, para la contratación de las auditorías externas de TI.			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	**[529]COOPEFYL** Debe revisarse la aplicación de este artículo a la luz de lo que	**[229] No procede** Las disposiciones señalan que las entidades y empresas supervisadas	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:	establece el artículo 3 del presente reglamento y lo definido en el anexo 2 de los lineamientos generales ya que están en contraposición.	sujetas a la aplicación del artículo 3 deben remitir el perfil tecnológico, y revelar en este los procesos de evaluación del marco de gobierno y gestión de TI, los cuales, deben estar en consonancia con los indicados en el anexo 2.	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.	**[530]COOPEANDE** 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. Con base en el alcance y niveles de capacidad definidos por la Entidad para dichos procesos. e) Proveedores de bienes y servicios de TI que, según los riesgos identificados, requieran la evaluación de una auditoría externa de TI. Valorar casos donde fabricantes de clase mundial no permitan recibir una auditoría puntual solicitada por la Entidad, para esto los fabricantes tienen evaluaciones y auditorías que hacen públicas y que cumplen con las buenas prácticas.	**[530] No procede** Se ajustó la redacción para aclarar las disposiciones con parte de los comentarios de la observación. 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.	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.
	[531]FEDEAC 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. Con base en el alcance y niveles de capacidad definidos por la Entidad para dichos procesos. e) Proveedores de bienes y servicios de TI que, según los riesgos	**[531] No procede** Se ajustó la redacción para aclarar las disposiciones con parte de los comentarios de la observación. 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.	

	identificados, requieran la evaluación de una auditoría externa de TI. Valorar casos donde fabricantes de clase mundial no permitan recibir una auditoría puntual solicitada por la Entidad, para esto los fabricantes tienen evaluaciones y auditorías que hacen públicas y que cumplen con las buenas prácticas. Definir la gradualidad de aplicación de los nuevos procesos.		
	[532]COOPEBANPO Esto es un comentario al margen de lo que establece este articulo: la práctica actual, debido a que hay una norma que cumplir es que los auditores se basan en evaluar el marco de gestión pero su enfoque es que la SUGEF no les cuestione los informes, entonces en las entidades nos hemos topado con auditores que no se animan a justificar que un proceso no aplica solo para que la sugef no les cuestione el informe final, así, Uds. se van a encontrar entidades pequeñas que tienen dentro de su marco de gestión 34 procesos que a todas luces es evidente que habrá mucho que por su naturaleza no les aplican. Adicionalmente hay que entender que entre más procesos tiene una entidad en su marco de gestión, más cara es la auditoria, con la incorporación de todas estas normas de ciberseguridad es un hecho cierto que el costo de estas auditorias va a subir de manera importante.	**[532] No procede** Se modificó la matriz de evaluación de auditores externos a fin de mitigar aspectos como los indicados.	
	[533]CAJAANDE	**[533]No procede**	

	Si se gestionara de manera corporativa, no queda claro si las auditorías deben realizarse por separado y presentar un informe por separado.	El artículo 47 indica entre otras disposiciones que 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. En la práctica, usualmente se remite un solo informe, con una visión integral y con las particularidades específicas de cada una de las entidades y empresas supervisadas del grupo.	
	[534]VIDAPLENA Los lineamientos establecen todos los procesos/objetivos de COBIT 2019, para entidades supervisadas que ya tienen definido su Marco de Gestión Personalizado, en este caso. ¿La Auditoría Externa se va a limitar a auditar los objetivos establecidos que la empresa ha establecido dentro de ese marco, o va a Auditar todos los procesos indicados en los lineamientos? La redacción sobre lo mencionado en el punto a) podría mejorar.	**[534] No procede** En el artículo 43 se establece que la entidad debe incluir en el perfil de TI los procesos de evaluación que le son aplicables. El articulo Artículo 47. Alcance y plazo de la auditoría externa de TI indica que las Superintendencias deben comunicar a las entidades y empresas supervisadas, el alcance de la auditoría externa de TI, el cual podrá considerar entre otros 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.	
	[535]BCR Pregunta ¿Supone este artículo que sea el Comité de TI quien defina formalmente el alcance de la Auditoría Externa?	**[535]No procede** Se atiende como consulta. El articulo Artículo 47. Alcance y plazo de la auditoría externa de TI indica que las Superintendencias deben comunicar	

		a las entidades y empresas supervisadas, el alcance de la auditoría externa de TI, el cual podrá considerar entre otros 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.	
	[536]CCPA Consideramos importante observar el Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Trabajos para Atestiguar y Servicios Relacionado adoptado por el Colegio, y realizar alguna sesión especifica con el Colegio para que esta sección contemple las perspectivas del contador público autorizado quien es el que realiza este tipo de trabajos.	**[536] No procede** Se ajustó la redacción para indicar lo siguiente: 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.	
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.		Se ajusta la redacción con parte de la observación del inciso e) del articulo 47 Alcance de la AE de TI	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.			f) El periodo de cobertura.
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			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.			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.			El plazo para la auditoría externa de TI y los canales de remisión del alcance están establecidos en los lineamientos generales del presente reglamento.
Artículo 48. Periodicidad de las auditorías externas de TI			**Artículo 48. Periodicidad de las auditorías externas de TI**
La periodicidad de la auditoría externa será cada dos años, excepto, cuando el supervisor considere con base en el perfil de riesgo o los resultados de la supervisión, la necesidad de anticiparla o aplazarla.	**[537]MUCAP** Analizar que cada dos años, genera una gran demanda de trabajo y que el próximo proceso de auditoría requiere 1 año hacia atrás de evidencia, y por lo tanto no habría tiempo para madurar controles, ya que el primer año se estaría atendiendo el plan de acción y el segundo año la auditoría.	**[537] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	La periodicidad de la auditoría externa será cada tres ~~dos~~ años, excepto, cuando el supervisor considere con base en el perfil de riesgo o los resultados de la supervisión, la necesidad de anticiparla o aplazarla.
	[538]COOPEMEP Se recomienda dejar el periodo de la normativa anterior.	**[538] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[539]FEDEAC ¿Se ha considerado el plazo que puede tardar la implementación de un plan de acción? ¿Cuál es el criterio para definir que el plazo mínimo de periodicidad debe ser de 2 años y no otro periodo? Un ciclo de 2 años no permite eficacia en el cumplimiento de planes. No hay necesidad de cambiar los plazos definidos actualmente.	**[539] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[540]CATHAY Nos parece que la periodicidad de la auditoría externa de 2 años es muy poco tiempo entre una y otra,	**[540] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	

	tomando en cuenta el volumen de procesos que se evalúan, se emplean 9 meses en el proceso de auditoría lo que dejaría un espacio cercano a un año para presentar planes de acción y ejecutarlos para cumplir con los planes de cumplimiento solicitados por la superintendencia.		
	[541]AAP Se considera este punto como el segundo punto más prioritario del reglamento. Favor considerar dejar el periodo de la normativa anterior. Se considera muy estrecho tomando en cuenta la carga operativa actual, los compromisos normativos y la auditoría en ese plazo. Tomando en consideración la experiencia vivida, los procesos de auditoría resultan intensivos para los equipos de trabajo, tomando en cuenta los plazos de auditorías y plan de acción, los supervisados estarían potencialmente en auditoria de manera permanente, lo que agota los recursos para trabajar en la operativa. Por tanto, se considera prudente conservar los plazos según reglamento anterior 5-17. "El intervalo entre una y otra no puede ser menor a dos años ni mayora cuatro años"	**[541] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[542]BAC La auditoría externa para la Corredora de Seguros quedó en un plazo diferente que para el resto de las entidades supervisadas. ¿Es posible que las entidades podamos	**[542] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	

	solicitar que las auditorias queden alineadas?		
	[543]CAJAANDE Se recomienda que la periodicidad debe mantenerse de acuerdo a lo que se indicaba Sección II: del reglamento GENERAL DE GESTIÓN DE LA TECNOLOGÍADE INFORMACIÓN SUGEF 14-17 Auditoría Externa de TI "El intervalo entre una y otra solicitud no puede ser menor a dos años ni mayor a cuatro años, excepto, cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de adelantarla", debido a que actualmente las instituciones financieras están obligadas a llevar varias auditorias, lo cual equivale a mayores cargas económicas y laborales.	**[543] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[544]COOPEALIANZA Dado el esfuerzo en recursos financieros, humanos y de tiempo que conlleva realizar auditorías de este tipo y dado el incremento de procesos a implementar en este nuevo reglamento, se solicita ampliar la periodicidad de la auditoría externa a tres años.	**[544] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[545]VIDAPLENA ¿A partir de qué momento, se calcula la aplicación de los dos años? Existen claras diferencias entre las auditorias de TI; en relación con las auditorias financieras y las de LC/FC. Los tiempos que se han observado entre la entrega de la	**[545] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	

	documentación al Ente Supervisor por parte de la firma auditora y que el Ente Supervisor "acepte" la Auditoría realizada, pueden pasar hasta seis meses; y hay que considerar además el plazo para cumplir con los planes de acción, lo cuales depende de la complejidad del proceso que se tiene que realizar para cumplir con el nivel solicitado que se ha definido.		
	[546]POPULARPENSIONES El plazo entre las auditorías es extremadamente corto, especialmente si se tiene en cuenta que la contratación y ejecución de cada Auditoría Externa es de nueve meses, adicionalmente se deben realizar las presentaciones a los entes supervisores y generar los planes de acción. Se considera que lo estipulado en el artículo 11 del Reglamento anterior, donde la periodicidad establecida se encontraba entre 2 y 4 años, se debe conservar.	**[546] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[547]ABC La periodicidad de 2 años establecida implica un costo significativo, máxime que se requiere de una firma de auditoría con especialistas en gestión y en ciberseguridad. Adicionalmente, dicho plazo podría afectar la atención de hallazgos de las auditorías previas. Por otro lado, las auditorías de las corredoras de seguro deberían estar alineadas con estos plazos.	**[547] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación. .	
	[548]OPC-CCSS	**[548] Procede**	

	Se indica que la periodicidad de la auditoría externa será cada dos años, sin embargo, se considera que este plazo es relativamente pequeño y deberían hacerse en un plazo mayor. La atención de las auditorías es un proceso que conlleva mucho tiempo, desde su planificación, contratación de la empresa auditora, ejecución y posteriormente la atención de los planes de acción, por lo cual no existiría ese margen para que las empresas ejecuten sin atrasos o cargas laborales excesivas, sus tareas operativas y mejora continua de los procesos.	Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[549]CB Es importante señalar que realizar estas auditorías cada 2 años no solo genera una gran demanda de trabajo, sino que además el próximo proceso de auditoría requiere 1 año hacia atrás de evidencia, y por lo tanto, no habría tiempo para madurar controles, ya que el primer año se estaría atendiendo el plan de acción y el segundo año la auditoría. Adicionalmente, el plazo considerado podría afectar la atención de hallazgos de las auditorías previas.	**[549] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[550]SEGUROSLAFISE Se considera este punto como el segundo punto más prioritario del reglamento. Favor considerar dejar el periodo de la normativa anterior. Se considera muy estrecho tomando en cuenta la carga operativa actual, los	**[550] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	

	compromisos normativos y la auditoría en ese plazo. Tomando en consideración la experiencia vivida, los procesos de auditoría resultan intensivos para los equipos de trabajo, tomando en cuenta los plazos de auditorías y plan de acción, los supervisados estarían potencialmente en auditoria de manera permanente, lo que agota los recursos para trabajar en la operativa. Por tanto, se considera prudente conservar los plazos según reglamento anterior 5-17. "El intervalo entre una y otra no puede ser menor a dos años ni mayora cuatro años"		
	[551]COOPENAE Por el esfuerzo, en no solo implementar 6 procesos adicionales, sino también porque se requieren certificaciones externas, lo cual implica, entre otras cosas, revisión de la estructura organizacional, gestión de talento (profesionales capacitados y actualizados) y nivel de madurez de las entidades, solicitamos a la SUGEF, considerar mantener los plazos actuales de las auditorías entre 2 a 4 años.	**[551] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[552]BCR • ¿La auditoría se deberá realizar siempre por solicitud expresa del supervisor o de oficio se hace cada 2 años aún y cuando ningún supervisor lo solicite? • Valorar un plazo más extendido de 2 años, por las siguientes razones:	**[552] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	

	o La inversión económica en la que el Conglomerado debe incurrir tanto en Banco como en Subsidiarias. o El costo operativo que esto implica cuando el marco es corporativo, dado que involucra tanto a Banco como a Subsidirias, áreas de TI, de negocio y órganos de dirección. o Tiempo óptimo para que los procesos puedan avanzar en su nivel de madurez.		
	[553]CIS Se recomienda dejar el periodo de la normativa anterior	**[553] Procede** Se ajusta la disposición, considerando parte de lo señalado en la observación.	
	[554]ISACA Las auditorías externas de TI para este reglamento deben tener la periodicidad de estándares rigorosos de la industria de Tarjetas de Pago, cuya periodicidad es trimestral, revisión interna demostrable y evidenciable, para una revisión anual que compila las 4 revisiones trimestrales. Así como el nicho de mercado de las tarjetas de pago es tan vulnerable, lo mismo son los servicios tecnológicos financieros que prestan y ejecutan las entidades.	**[554] No Procede** Se ajusta las disposiciones del artículo, considerando parte de la observación [537].	
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:	**[555]CCPA** Consideramos importante observar el Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría,	**[555] No procede** Se ajusta la disposición, considerando parte de lo señalado en la observación [519]	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:

	Revisión, Otros Trabajos para Atestiguar y Servicios Relacionado adoptado por el Colegio, y realizar alguna sesión especifica con el Colegio para que esta sección contemple los requerimientos de la normativa mencionada.		
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.	**[556]MUCAP** No existe claridad a qué se refiere con el "encargo".	**[556] 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. La planificación del encargo es una actividad usual que deben realizar los auditores certificados CISA, como parte de su labor y según lo establecido en el ITAF del ISACA.	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:	**[557]COOPENAE** 1-(Impacto Alto, Esfuerzo Alto). Se le solicita un nuevo producto llamado "planificación del encargo de la auditoría externa de TI", donde el auditor externo tiene 20 días hábiles luego de la firma del contrato para presentarlo a la	**[557] No procede** La planificación del encargo es una actividad usual que deben realizar los auditores certificados CISA, como parte de su labor y según lo establecido en el ITAF del ISACA. 2-Se ajustó la disposición, considerando parte de lo señalado en la observación [537].	Las entidades y empresas deben remitir a la respectiva Superintendencia los siguientes productos de la auditoría externa de TI:

	entidad y esta a su vez remitirlo al regulador. 2-Los plazos de las auditorías estaban espaciados entre 2 y 4 años, pero se reducen a cada 2 años, lo cual brinda poco margen para poder implementar los nuevos procesos, entendiéndose que a nivel de ciberseguridad y plataformas "cloud" se requiere de certificaciones externas. Asimismo, los plazos de planes de acción y seguimiento se fijan en cada 6 meses su actualización.		
	[558]CCPA Consideramos importante observar el Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Trabajos para Atestiguar y Servicios Relacionado adoptado por el Colegio, y realizar alguna sesión especifica con el Colegio para que esta sección contemple los requerimientos de la normativa mencionada.	**[536] No procede** Se ajustó la disposición, considerando parte de lo señalado en la observación [519].	
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.			c)La matriz de evaluación del marco de gobierno y gestión de TI.
d)Cualquier otro producto solicitado por la Superintendencia en el alcance de la auditoría externa de TI.			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 auditoría externa de TI por parte del auditor CISA responsable.			Las entidades y empresas supervisadas deben convocar, previa coordinación con la respectiva Superintendencia, una reunión para la presentación de los resultados de la auditoría externa de TI por parte del auditor CISA responsable.
Los canales para la coordinación de la reunión, el contenido mínimo de la presentación de los resultados de la auditoría externa de TI y las personas que deben participar están establecidos en los lineamientos generales del presente reglamento.			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.	**[559]FEDEAC** ¿Se desprende de este artículo que la supervisión de este reglamento recae sobre la Auditoría Externa, qué supervisión basada en riesgos aplicará SUGEF, puesto que en el acuerdo SUGEF 24-22 no se incluye una guía o apartado específico para la evaluación de TI o de Riesgo de TI?	**[559] No procede** 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 Por otra parte, en los anexos del Acuerdo SUGEF 24-22 se hace referencia al tema de tecnología de información como parte de los elementos y criterios de evaluación.	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.
	[560]BCR 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,	**[560] No procede** Este es un plazo máximo que está en función de la complejidad de los hallazgos en la entidad.	

	además de los costos de contratación del auditor externo.		
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.			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.	**[561]MUCAP** No queda claro si la entidad puede recurrir esa decisión del supervisor de conformidad con la Ley General de la Administración Pública; solo está regulado lo de la prórroga del plazo.	**[561] No procede** Las disposiciones del presente reglamento no contravienen lo establecido en normas de orden superior como lo es la Ley de Administración pública.	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.
	[562]FEDEAC Valorar si el plazo de 30 días hábiles es aceptable cuando la Superintendencia cuanta con 40 días hábiles para remitir el reporte de supervisión. El plazo debería ser equivalente al del artículo 52.	**[562] No procede** El plazo dispuesto se estableció de conformidad con lo establecido en otras normas vigentes aprobadas por el CONASSIF, las cuales, consideran la elaboración de planes de acción.	
	[563]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 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.	**[563] No Procede** 1-La disposición indica que cuando se incumplan las disposiciones establecidas en este reglamento, en sus lineamientos generales o en ambos, el supervisor puede declarar inadmisibles los productos de la auditoría externa de TI. 2-Este plazo de diez días es en caso de cambios menores que no requieran los 30 días.	
En caso de inadmisibilidad, las entidades o empresas supervisadas deben remitir los productos corregidos en			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 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.	**[564]OPC-CCSS** 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.	**[564] No Procede** EL articulo 52 indica los plazos en los que la superintendencia podrá remitir el reporte de supervisión, en este caso 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.	El plazo dispuesto para que las Superintendencias remitan nuevamente el reporte de supervisión iniciará a partir de la última recepción de los productos corregidos.
Las Superintendencias pueden solicitar una nueva reunión para la presentación de los resultados finales de la auditoría externa de TI.			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 auditoría externa de TI.	**[565]OPC-CCSS** 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.	**[565] No Procede** La disposición indica que 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. Se incluye texto para mejorar el entendimiento de la disposición.	Las entidades y empresas supervisadas deben elaborar un plan de acción para gestionar los hallazgos y los riesgos que se identifiquen como resultado de la auditoría externa de TI. Las acciones que se incluyan en el plan de acción deben establecerse en función del tamaño, complejidad y modelo de negocio, así como de los niveles de apetito, tolerancia y capacidad de riesgo establecidos.
La aprobación de los planes de acción por parte del supervisor aplicará en aquellos casos en los que así lo defina la regulación específica de cada Superintendencia.			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.			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.	**[566]FEDEAC** Valorar si el plazo de 30 días hábiles es aceptable. El plazo debería ser equivalente al del artículo 52.	**[566] Procede** Se revisan los plazos y se ajusta, considerado la observación [562].	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.
	[567]BCR El plazo de elaboración del plan de acción debería ampliarse al menos a 40 días hábiles, La elaboración del plan de acción requiere de la participación de todas las áreas involucradas en las acciones que se definan, mismas que además deben atender su día a día, revisión y análisis de impacto en planes estratégicos, operativos y tácticos, además considerar, el tiempo de aprobación en los diferentes órganos de dirección (Comité Corporativo Ejecutivo, Comité Corporativo de TI, Juntas Directivas),	**[567] No procede** El plazo dispuesto en la presente modificación reglamentaria está conforme a lo establecido en otras normativas vigente aprobadas por el CONASSIF, relacionadas con los 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.	**[568]INS** Se estima que es prudente, establecer la dimensión y complejidad de la entidad supervisada, como un elemento importante para otorgar las	**[568] No procede** Las prórrogas se establecen de conformidad con lo establecido en la ley general de administración pública.	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.

	prórrogas, así como establecer que dichas prorrogar deben ser proporcionales a la dimensión de la empresa supervisada.		
	[569]CFBNCR 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.	**[569] No procede** Las prórrogas se establecen de conformidad con lo establecido en la ley general de administración pública.	
	[570]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, se solicita establecer un plazo para la respuesta por parte del Regulador	**[570] No procede** Las prórrogas se establecen de conformidad con lo establecido en la ley general de administración pública.	
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.	**[571]OPC-CCSS** Se sugiere incluir un periodo de tiempo para que el supervisor indique si está de acuerdo o no con las solicitudes de prórrogas, para que la empresa esté enterada y planifiquen actividades a nivel interno considerando esas fechas.	**[571] Procede** Se ajusta el texto, de conformidad con la resolución (Resolución n.° 643-1993 del 8 de febrero de 1993) de la Procuraduría General de la República, la cual entre otros aspectos indica que: Plazo para contestar Resumen del contenido: Plazo legal para dar respuesta, Entrega inmediata de información de interés público o en menor tiempo posible, Extensión del plazo en solicitudes complejas, Deber de informar motivos	La respectiva Superintendencia valorará los fundamentos presentados en la solicitud de prórroga y aceptará o rechazará dicha solicitud.

		de retraso y tiempo estimado de respuesta, Supuestos que suspenden plazo, Acceso inmediato de partes a expedientes administrativos. El plazo de 10 días hábiles previsto en el artículo 32 de la LJC es de aplicación para la respuesta de las solicitudes de información. "(…) De conformidad con lo dispuesto en el artículo 32 de la Ley de la Jurisdicción Constitucional, cuando el amparo se refiera al derecho de petición y de obtener pronta resolución, establecido en el artículo 27 de la Constitución Política y no hubiere plazo señalado para contestar, se entenderá que la violación se produce una vez transcurridos 10 días hábiles desde la fecha en que fue presentada la solicitud en la oficina administrativa, sin perjuicio de que en la decisión del recurso se aprecien las razones que se aduzcan para considerar insuficiente ese plazo, atendidas las circunstancias y la índole del asunto.	
En caso de aceptación de la solicitud, se comunicará a la entidad o empresa supervisada el plazo adicional concedido mediante los canales oficiales de comunicación de cada Superintendencia.		Se modifica el párrafo de conformidad con lo resuelto en la observación [571].	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 ~~mediante los canales oficiales de comunicación de cada Superintendencia~~. 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	**[572]OPC-CCSS** El regulador no consideró ninguna disposición transitoria para la adecuación del marco de gobierno	**[572] Procede** Se incluyó una disposición transitoria relacionada con identificación 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.	y gestión de TI de los regulados lo cual supone un nulo tiempo de acción para atender la regulación que tiene un alto impacto en cambios a nivel de procesos de negocio, técnicos y de fiscalización de las líneas de defensa, lo cual supondría incumplimiento inmediato por parte de todos los entes que no cumplan con la totalidad de aspectos señalados en el reglamento propuesto.	brechas e implementación de las disposiciones reglamentarias.	Información, Acuerdo CONASSIF 5-17, debe leerse como Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24.
	[573]CB 1- El Reglamento no contempla un plazo de "vacatio legis" para que las entidades se adapten a las nuevas obligaciones. Es una realidad que la cantidad y complejidad de los nuevos requerimientos implican una cantidad importante de inversiones, cambios en el gobierno corporativo y adopción de nuevas tecnologías, nuevos procesos y políticas que es imposible cumplir de forma inmediata. En tal sentido, se solicita un plazo mínimo de 1 año para la entrada en vigor del Reglamento, a partir de su publicación. 2-No queda claro si lo que se indica es que los contratos vigentes con proveedores de TI no podrán seguir rigiéndose por el anterior Reglamento, más de 12meses después de la entrada en vigor de dicho Reglamento, a pesar de que el contrato venza en	**[573]No procede** 1-Respecto al punto 1, se aclara que se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias. 2-Respecto al punto 2, no procede. Se incluye en el transitorio "Contratos con proveedores de bienes y servicios de TI", la disposición 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. 3-Las facultades y responsabilidades de las superintendencias se encuentran definidas en otras leyes y reglamentos, razón por la cual no se incluyen en las disposiciones de la presente propuesta. 4- Respecto al punto 4, se aclara que se incluyó una disposición transitoria relacionada con identificación de	

	una fecha posterior a esos 12 meses. De ser así, es recomendable respetar en la medida de lo posible los plazos contractuales, pues de lo contrario podrían darse responsabilidades legales y pecuniarias paralas entidades. 3-TEMAS ADICIONALES Confidencialidad de la información: Con este Reglamento, SUGEF manejará una cantidad importante de información sensible, acerca de la seguridad de las entidades, los datos de sus clientes, secretos comerciales, entre otra. Congruente con ello, se solicita incluir en este Reglamento, disposiciones sobre las obligaciones que asumen las Superintendencias para proteger esa información, más allá de las regulaciones ya existentes y aplicables. 4-Impacto en la innovación: La carga regulatoria del nuevo reglamento es considerable. En tal sentido, 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. Se debe buscar un equilibrio entre la seguridad de la información y la innovación tecnológica, la cual requiere del aprovechamiento responsable de los datos. ////////////////////////////////Comentarios a	brechas e implementación de las disposiciones reglamentarias. 5-La entrada en vigor de las modificaciones reglamentarias no interrumpe el ciclo de auditorías, ni el desarrollo de los planes de acción vigentes.	

	5-Disposición adicional primera. Referencias normativas Se estima que si la auditoría externa es de fecha previa a la entrada en vigencia de esta normativa (en el año previo), no debería solicitarse auditorías adicionales, sino hasta cumplir el plazo de dos años a partir de la entrada en vigencia de esta normativa, ya que se le estaría dando un efecto retroactivo a la Normativa CONASSIF 5-24 sobre la SUGEF 5-17 y entra en contradicción con el Transitorio III.		
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.	**[574]MUCAP** El transitorio debería enfocarse en que, si la auditoría externa es de fecha previa a la entrada en vigencia de esta normativa (en el año previo), no debería solicitarse auditorías adicionales, sino hasta cumplir el plazo de dos años a partir de la entrada en vigencia de esta normativa, ya que se le estaría dando un efecto retroactivo a la Normativa CONASSIF 5-24 sobre la SUGEF 5-17 y entra en contradicción con el Transitorio III Adicionalmente, el efecto sobre el costo en contratos ya firmados. La aplicación de la normativa CONASSIF 5-24 afectará irremediablemente el costo ya pactado en los contratos en ejecución.	**[574] No Procede** La entrada en vigor de las modificaciones reglamentarias no interrumpe el ciclo de auditorías, ni el desarrollo de los planes de acción vigentes.	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.

	Como complemento se hace mención que el presupuesto para los contratos en ejecución ya está determinado por la entidad, por lo que habría que estimarse el costo adicional indicado en el punto anterior.		
	[575]FEDEAC Para las auditorías en marcha no solo deben respetarse los plazos sino también los procesos o alcance de trabajo ya definidos. Definir si las CACs bajo el Acuerdo SUGEF 25-23 deben ajustar los trabajos en marcha a los procesos aquí aplicados en proporcionalidad.	**[575] No Procede** La entrada en vigor de las modificaciones reglamentarias no interrumpe el ciclo de auditorías, ni el desarrollo de los planes de acción vigentes.	
	[576]AAP Se considera el punto de la creación de nuevos transitorios para implementación de estos reglamentos, como el primer punto y más prioritario del reglamento.	**[576] Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	
	[577]FECOOPSE Para el caso de las cooperativas sujetas a la normativa de regulación proporcional (SUGEF 25-26) se pone en evidencia la necesidad de contar con un marco normativo de TI acorde a su naturaleza jurídica, tamaño, perfil de riesgo, enfoque de negocio, volumen y complejidad de operaciones, es decir proporcional, lo cual tiene consideraciones claras respecto a costos, carga regulatoria y otros criterios (ver SUGEF 25-23 Consideraciones sobre proporcionalidad).En la hoja de	**[577] No Procede** La entrada en vigor de las modificaciones reglamentarias no interrumpe el ciclo de auditorías, ni el desarrollo de los planes de acción vigentes.	

	ruta esta normativa ha tenido varias fechas para su aprobación y aun así se cuentan con solicitudes de auditoría en proceso que no responden a dicha proporcionalidad, es decir, bajo el enfoque anterior, lo cual tiene un impacto en costos que se contrapone a las consideraciones sobre proporcionalidad supra citadas. El 23 de agosto del 2023 se realiza la presentación del acuerdo 25-23 a las cooperativas sujetas a dicha norma, en esta presentación se indica en las observaciones, punto 4, que la propuesta hecha por FECOOPSE en mayo 2023 se está incluyendo en la reforma integral de la normativa 5-17, por lo que el alcance se acota al propuesto por FECOOPSE, es decir, 13 procesos. Ante la consulta: "Se indica que se está considerando la proporcionalidad para la aplicación de CONASSIF 5-17, pero posterior a la consulta emitida desde FECOOPSE varias cooperativas recibimos el requerimiento para la aplicación de la auditoría de 34 procesos. ¿Para cuándo se tendría claridad sobre los alcances proporcionales sin que ello implique asumir costos demás?", a lo que se respondió que en hoja de ruta se tiene que para finales de septiembre 2023 se enviará a consulta al sector financiero el nuevo enfoque que incluye la proporcionalidad antes		

	mencionada, adicionalmente se indica que a nivel de transitoriedad se aplicará igual que la entrada en vigencia del acuerdo 25-23,por lo que una vez que entren en vigencia los nuevos cambios, la existencia de informes de regulación, requerimientos y hallazgos; automáticamente quedan adaptados al nuevo enfoque una vez sea aprobada la nueva norma de TI. (Verhttps://bccr.webex.com/recordingservice/sites/bccr/recording/cec59308241a103cabde9e06991c68f3/playback (contraseña gCXAaCV8), ver minutos: 57 y 92.)Por lo tanto: se recomienda excluir a las cooperativas sujetas a la normativa SUGEF 25-23 de este transitorio dado que en estos casos en particular el alcance de la nueva normativa se adecua a los términos de proporcionalidad.		
	[578]ABC Es necesario contar con un plazo prudencial para la implementación de las obligaciones contenidas en el Reglamento propuesto, por lo que se solicita un plazo mínimo de 1 año a partir de la publicación para que entre en vigencia la normativa. Lo anterior considerando que los nuevos requerimientos implican una cantidad importante de inversiones, cambios en el gobierno corporativo y adopción de nuevas tecnologías, proceso y políticas cuyo cumplimiento inmediato no es factible.	**[578] Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	

	[579]SEGUROSLAFISE Se considera el punto de la creación de nuevos transitorios para implementación de estos reglamentos, como el primer punto y más prioritario del reglamento.	**[579] Procede** Se incluye una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	
	[580]ISTMO Al no existir un transitorio, que pasaría con una solicitud de Auditoría, ésta tendría únicamente un alcance basado en reglamento anterior? ¿O se solicitarán con un alcance limitado a los temas del marco de gestión, con el objetivo de dar tiempo a las empresas supervisadas para que adopten todos los nuevos elementos que contempla el nuevo reglamento?	**[580] No Procede** La entrada en vigor de las modificaciones reglamentarias no interrumpe el ciclo de auditorías, ni el desarrollo de los planes de acción vigentes.	
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.	**[581]FEDEAC** Los Planes de Acción en curso de CACs bajo el Acuerdo SUGEF 25-23 deben ajustarse a los procesos aquí aplicados en proporcionalidad.	**[581] No Procede** 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. Dicha matriz se encuentra a disposición de las entidades.	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:			Con respecto a los contratos vigentes y futuros suscritos con los proveedores de bienes y servicios de TI, las entidades y empresas supervisadas deben considerar lo siguiente:
a) Contratos nuevos: A partir de la publicación de las modificaciones del presente reglamento en el diario oficial La Gaceta, deben acatarse las disposiciones sobre contratos y acuerdos de nivel de servicio.			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.	**[582]MUCAP** Con relación al numeral b) sobre contratos vigentes, se genera un riesgo muy grande si existirá el espacio de negociación con proveedores en contratos ya vigentes, para aplicar lo dispuesto en esta Normativa; ya que esto constituye un criterio de retroactividad de la nueva normativa con respecto al Acuerdo 5-17, tal y como se hizo en comentario al Transitorio I Adicionalmente, considerar el efecto sobre el costo en contratos ya firmados. La aplicación de la normativa CONASSIF 5-24 afectará irremediablemente el costo ya pactado en los contratos en ejecución Se puede indicar también que el presupuesto para los contratos en ejecución ya está determinado por la entidad, por lo que habría que estimarse el costo adicional indicado en el punto anterior Finalmente se debería indicar la observación que los contratos vigentes no deben ajustarse sino hasta su vencimiento, por el principio de no retroactividad.	**[582] Procede** Se aclara que el principio de no retroactividad, no se está violentando al brindarle un plazo de 12 meses indicados en la propuesta de forma inicial, lo anterior, con el fin de pactar las nuevas condiciones. Se adiciona en la disposición que, en casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.	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.

	[583]COOPEBANPO Considerar eliminar el requerimiento de los doce meses, pues podría haber contratos firmados a mayor tiempo que doce meses. eso obligaría a renegociar o dar por terminado un contrato si las partes no se ponen de acuerdo. Los convenios ya establecidos deberían respetarse y la superintendencia no debería obligar a las entidades a renegociar actos que están formalizados.	**[583] No procede** Se adiciona en la disposición que, en casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.	
	[584]BAC Se solicita ampliar el plazo para los ajustes en temas contractuales (con los actuales proveedores) de al menos 24 meses luego de su publicación en la gaceta.	**[584]No procede** Se adiciona en la disposición que, en casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.	
	[585]INS En la disposición transitoria cuarta, denominada contratos con proveedores de bienes y servicios de TI, se establece un inciso b), según el cual los contratos vigentes a la fecha de entrada en vigor del reglamento se mantendrán según lo pactado entre las partes, pero en caso de renovación y nuevos contratos se deberán ajustar a la nueva normativa; sin embargo, también establece que el plazo no podrá exceder de doce meses. En primer lugar, la frase "dicho plazo" resulta imprecisa, pues en los párrafos precedentes no se menciona ningún término, por lo que no hay claridad respecto al plazo del que se trata. Ahora bien,	**[585] No procede** Se adiciona en la disposición que, en casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.	

	en el supuesto de que se refiera al plazo máximo durante el cual se podrán mantener vigentes los contratos en las mismas condiciones; se estima que la norma debe hacer una excepción razonable para aquellas empresas públicas o estatales que están sujetas a la contratación pública, pues las modificaciones en dicho régimen de contratación tienen sus propias reglas específicas, especialmente tomando en consideración que dichas contrataciones ya fueron pactadas por plazos y prorrogas previamente establecidos y acordados por las partes, por lo que si el proveedor no está de acuerdo en realizar la modificación deberá acudirse a otro proceso de contratación que puede resultar muy complejo y sería más gravoso para la entidad no contar con el servicio contratado.		
	[586]VIDAPLENA Es importante considerar, que esto aplicaría en el caso de contratos que NO son de adhesión.	**[586] No Procede** Aplica para todo tipo de contrato.	
	[587]CFBNCR 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	**[587] Procede** Se ajusta la redacción para aclarar la disposición.	

	para analizar su viabilidad y razonabilidad.		
	[588]ABC Es preciso aclarar a qué se refiere el plazo de los 12 meses: al plazo de renovación de contratos preexistentes o al plazo de los nuevos contratos.	**[588] Procede** Se ajusta la redacción para aclarar la disposición.	
	[589]OPC-CCSS La redacción en nuestro criterio se presenta ambigua en la medida en que no queda claro si la pretensión es que la suscripción de contratos con proveedores de bienes y servicios de TI, nuevos o renovaciones, tendrá que ser por un plazo de como máximo doce meses. Lo anterior, se contrapone a loque permite la Ley General de Contratación Pública, Nº 9986 que en su artículo 104 dispone: "ARTÍCULO 104- Plazo El plazo ordinario del contrato no podrá superar el término de cuatro años, considerando el plazo original y sus prórrogas. En casos excepcionales, en atención a las particularidades del objeto contractual, o la modalidad de contratación en las que se requiera un mayor plazo para recuperar la inversión, podrá recurrirse a vigencias contractuales superiores a dicho plazo máximo. Para acordar un plazo mayor a cuatro años, desde la decisión inicial deberá estipularse la posibilidad de vigencias contractuales superiores, con indicación del plazo máximo para la contratación particular, previa resolución	**[589] No Procede** Se aclara que el principio de no retroactividad, no se está violentando al brindarle un plazo de 12 meses indicados en la propuesta de forma inicial, lo anterior, con el fin de pactar las nuevas condiciones. Se adiciona en la disposición que, en casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.	

	motivada suscrita por el jerarca en donde se consignen las razones de la necesidad de una vigencia mayor sustentada en los estudios técnicos, financieros y jurídicos pertinentes suscritos por funcionarios competentes que así lo justifiquen. En cualquier caso, el plazo de la contratación no podrá superar los diez años. Queda a salvo lo establecido en el artículo 79 de la presente ley…" Como puede verse la Ley General de Contratación Pública, Nº 9986 permite a las Administraciones Públicas suscribir contratos administrativos para el aprovisionamiento de bienes y servicios hasta por un plazo máximo de 4 años dependiendo de las características y condiciones de la necesidad que se debe atender. Inclusive, la Administración contratante podría, en casos excepcionales y a través de un acto motivado, suscribir contratos por plazos mayores a 4 años cuando la modalidad de contratación requiera un mayor plazo para recuperar la inversión, lo cual podría darse en algún caso de contrataciones de proveedores de bienes y servicios de TI como las que refiere el proyecto de reglamento sometido a consulta. De ahí que puntualmente consultamos: 1. ¿Cómo debe interpretarse la disposición transitoria cuarta con respecto al plazo máximo de los contratos a suscribir con proveedores de		

	bienes y servicios de TI? ¿La disposición transitoria cuarta entendemos que no está obligando a rescindir contratos que actualmente estén vigentes y que sean por plazos mayores a doce meses? 2. ¿Está planteando el Reglamento un plazo máximo de doce meses para la vigencia de estos contratos, contrario a lo que dispone la Ley General de Contratación Pública, Nº 9986? 3. De ser la respuesta positiva, ¿cómo puede la Administración manejar casos en los que el objeto contractual y la modalidad de contratación requieran de plazos mayores a doce meses o inclusive a cuatro años, para efectos de recuperar la inversión en el negocio?		
	[590]CB Inciso b: Comentarios: 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 poder analizar su viabilidad y razonabilidad. En todo caso, para el caso de los contratos vigentes debe aclararse que estos no deben ajustarse sino hasta su vencimiento, por el principio de no retroactividad.	**[590] Procede** Se ajusta la redacción para aclarar la disposición	
	[591]BCR ¿Qué pasa si nuestras contrataciones no vencen en los	**[591] No Procede** Se aclara que el principio de no retroactividad, no se está violentando al	

	próximos 12 o 24 meses, cómo se establece los requerimientos contractuales solicitados, y si el proveedor no está de acuerdo y no puedo prescindir del servicio entonces, ¿qué sucede en estos casos?	brindarle un plazo de 12 meses indicados en la propuesta de forma inicial, lo anterior, con el fin de pactar las nuevas condiciones. Se adiciona en la disposición que, en casos debidamente justificados, podrán otorgarse prórrogas de hasta doce meses.	
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:	**[592]CAJAANDE** Se considera que se dé un plazo prudente (12 meses) para la entrada en vigencia, debido a la carga laboral que genera la implementación de estos temas.	**[592] Procede** Se incluyó una disposición transitoria relacionada con identificación de brechas e implementación de las disposiciones reglamentarias.	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:
Las sociedades corredoras de seguros deben implementar los procesos de su marco de gestión de TI gradualmente como máximo durante los primeros tres años contados a partir de la entrada en vigor del reglamento.		Se modificó a cuatro años de conformidad con lo indicado en las observaciones.	a) Las sociedades corredoras de seguros deben implementar los procesos de su marco de gestión de TI gradualmente como máximo durante los primeros ~~tres~~ cuatro años contados a partir de la entrada en vigor del reglamento.
En concordancia con la naturaleza, modelo de negocio, criticidad de los procesos y dependencia tecnológica de información y la complejidad de sus operaciones, la SUGESE requiere que las sociedades corredoras de seguros implementen su marco de gestión, así como los órganos, comités, instancias y controles, para lo cual deben contar con una estructura organizacional para la gestión de TI que delimite claramente sus obligaciones, funciones y responsabilidades y que cuente con políticas orientadas a cautelar una adecuada gestión de TI en congruencia con su estrategia de gestión de los riesgos de TI.			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, independientemente del tipo de gestión, comité o unidad de TI sea esta individual o corporativa que la entidad defina.			a) Las sociedades corredoras de seguros remitirán su primer perfil tecnológico de TI, a partir del 2025, independientemente del tipo de gestión, comité o unidad de TI sea esta individual o corporativa que la entidad defina.

b) Las fechas de remisión del primer perfil de las sociedades corredoras de seguros serán comunicadas por la SUGESE mediante acto administrativo en el tercer trimestre del 2024, a través de los canales oficiales.			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:
La SUGESE podrá requerir a las sociedades corredoras de seguros, la primera auditoría externa de TI a partir del enero del 2027.	**[593]CIS** En tal sentido, sería favorable al sector que se considere que al año 2027 es poco probable que se estén listos a capacidades altas que satisfagan los requerimientos de una auditoría externa, asumiendo que el camino es largo y está el compromiso de iniciar desde la entrada en vigencia de las n Es de interés verificar el entendimiento de que se pueden manejar diversos niveles de capacidades.	**[593] No procede** La disposición indica que SUGESE podrá requerir a las sociedades corredoras de seguros, la primera auditoría externa de TI a partir del enero del 2027.	La SUGESE podrá requerir a las sociedades corredoras de seguros, la primera auditoría externa de TI a partir del enero del 2027.
			Disposición transitoria sexta. Perfil tecnológico
		Se incluyó la disposición transitoria para aclar lo referente al perfil tecnológico mientras se incorporan en los sistemas las modificaciones reglamentarias.	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 generales. 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
		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 deben validar que cumplan con las disposiciones de la presente modificación reglamentaria; cuando presenten brechas deberán elaborar planes de implementación para atender dichas brechas.

			Las entidades y empresas supervisadas dispondrán de un plazo no mayor a tres años para finalizar los planes de implementación.
			Sin perjuicio de lo anterior, para la elaboración de los planes de implementación se deben considerar los plazos establecidos en los siguientes artículos de la modificación reglamentaria y en sus lineamientos generales, a fin de que la ejecución de los planes permita el cumplimiento de los plazos establecidos en dichos artículos:
			Artículo 39. Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias Artículo 40. Comunicado de incidentes a los clientes Artículo 41. Reporte histórico de incidentes Artículo 45. Comunicación de cambios significativos del perfil tecnológico Artículo 47. Alcance y plazo de la auditoría externa de TI Artículo 48. Periodicidad de las auditorías externas de TI
			Los planes de implementación deberán estar a disposición de las Superintendencias cuando estas lo requieran. Dichos planes podrán ser considerados para definir los alcances de la auditoría externa de TI o ser considerados como parte de la evaluación de las auditorías externas de TI.
Rige a partir de su publicación en el diario oficial La Gaceta.”			

CONTROL DE CORRESPONDENCIA					
Referencia	**Nombre del consultado**	**Alias**	**N°**	**Cantidad de**	**Cantidad de**

Sistema de Correspondencia			Observaciones	Observaciones "Procede"	Observaciones "No procede"
GGC-24-2024	Banco Popular de Desarrollo Comunal	BPDC	28	11	17
Oficio sin número de referencia	Cámara de Bancos e Instituciones Financieras de Costa Rica	CB	35	13	22
PE-GG-13783-2024	Cooperativa del Banco Popular	COOPEBANPO	21	6	15
GO-0008-2024	Bac Credomatic	BAC	10	3	7
SMS-TI-002-2024	SM Seguros	SMSEGUROS	4	0	4
2023020857	Caja de Ande	CAJAANDE	18	4	14
CISCR 00029-2024	Cámara de Intermediarios de Seguros de Costa Rica	CIS	16	6	10
ACOP-004-2024	Asociación Costarricense de Operadoras de Pensiones	ACOP	3	0	3
GG-04-2024	Vida Plena	VIDAPLENA	15	7	8
ABC-0005-2024	Asociación Bancaria Costarricense	ABC	27	13	14
GG-013-2024	Operadora de Pensiones Complementarias de la Caja Costarricense de Seguro Social	OPC-CCSS	22	8	14
GG-062-2024	Coopealianza	COOPEALIANZA	11	5	6
G-00147-2024	Instituto Nacional de Seguros	INS	5	1	4
AAP-E-001-2024	Asociación de Aseguradoras Privadas de Costa Rica	AAP	17	6	11
0014-2024	Federación de Cooperativas de Ahorro y Crédito	FEDEAC	41	12	29
GG-008-2024	Cooperativa Nacional de Educadores	COOPENAE	15	3	12
DE-0004-01-2024	Junta de Pensiones y Jubilaciones del Magisterio Nacional	JUPEMA	10	5	5
GG-161-2023	Cooperativa de Ahorro y Crédito de Los Empleados del Sector Público Privado e Independiente	COOPEFYL	16	0	16
No remitió oficio	Luis Diego León Barquero	Luis Diego León Barquero	40	15	25
No remitió oficio	Information Systems Audit and Control Association	ISACA	42	6	36
No remitió oficio	Banco de Costa Rica	BCR	36	9	27
No remitió oficio	Cooperativa de Ahorro y Crédito Ande	COOPEANDE	21	8	13
No remitió oficio	Colegio de Contadores Públicos de Costa Rica	CCPA	21	6	15
No remitió oficio	Banco Nacional de Costa Rica	BNCR7	7	1	6
GIR-006-2024	Conglomerado Financiero Banco Nacional de Costa Rica	CFBNCR	24	6	18
No remitió oficio	Cathay	CATHAY	12	5	7
No remitió oficio	Cooperativa de Ahorro y Crédito de los Servidores Públicos	COOPESERVIDORES	4	1	3
No remitió oficio	Aseguradora del ISTMO	ISTMO	11	4	7
No remitió oficio	Mutual Cartago Ahorro y Préstamo	MUCAP	25	13	12
No remitió oficio	Cooperativa de Ahorro y Crédito de los Empleados del Ministerio de Educación Pública	COOPEMEP	12	4	8

No remitió oficio	Popular Pensiones	POPULARPENSIONES	4	3	1
No remitió oficio	Seguros Lafise	SEGUROSLAFISE	18	7	11
No remitió oficio	Cámara de Intermediarios Bursátiles y Afines	CAMBOLSA	1	0	1
No remitió oficio	Federación de Asociaciones Cooperativas de Ahorro y Crédito	FECOOPSE	1	0	1
TOTAL			593	191	402