ACUERDO CONASSIF 5-24

REGLAMENTO GENERAL DE GOBIERNO Y GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante artículos 8 y 9 de las actas de las sesiones 1876-2024 y 1877-2024, celebradas el 15 de julio del 2024. Rige a partir de su publicación en el diario oficial La Gaceta. Publicado en el Alcance 130 a La Gaceta 134 del 22 de julio de 2024.

Versión documento	Fecha de actualización
1	5 de agosto de 2024

CONASSIF
Consejo Nacional de Supervisión del Sistema Financiero

TABLA DE CONTENIDO

CONASSIF
Consejo Nacional de Supervisión del Sistema Financiero

CONSIDERANDOS

El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 9 de las actas de las sesiones 1876-2024 y 1877-2024, celebradas el 15 de julio del 2024,

considerando que:

consideraciones de orden legal y reglamentario

I. El literal b) del artículo 171 de la Ley Reguladora del Mercado de Valores, Ley 7732, dispone, como una de las funciones del Conassif, aprobar las normas atinentes a la autorización, regulación, supervisión, fiscalización y vigilancia que, conforme a la ley, deben ejecutar la Superintendencia General de Entidades Financieras (Sugef), la Superintendencia General de Valores (Sugeval) y la Superintendencia de Pensiones (Supen). Asimismo, el artículo 28 de la Ley Reguladora del Mercado de Seguros, Ley 8653, dispone, en relación con la Superintendencia General de Seguros (Sugese), que: "al superintendente y al intendente les serán aplicables las disposiciones establecidas, de manera genérica y de aplicación uniforme, para las demás Superintendencias bajo la dirección del Conassif y sus respectivos superintendentes e intendentes".

II. El inciso d) del artículo 131 y el artículo 119 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558, confieren al Consejo Nacional de Supervisión del Sistema Financiero la potestad de dictar las normas generales que sean necesarias para el establecimiento de sanas prácticas bancarias de gobierno corporativo, incluidas las de idoneidad de miembros del Órgano de Dirección y puestos claves de la organización, así como de gestión de riesgos y de registro de las transacciones, entre otros aspectos, todo en salvaguarda del interés de la colectividad.

III. El inciso c) del artículo 131 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558, establece, como parte de las funciones del superintendente general de entidades financieras, proponer al Conassif, para su aprobación, las normas que estime necesarias para el desarrollo de las labores de supervisión y fiscalización.

IV. El artículo 3 de la Ley Reguladora del Mercado de Valores, Ley 7732, establece que la Sugeval debe velar por la protección del inversionista y la transparencia del mercado de valores. Asimismo, el artículo 8 de la Ley 7732, inciso b), establece que la Sugeval someterá a la consideración del Consejo Nacional los proyectos de reglamento que le corresponda dictar a la Superintendencia. El inciso j) establece la potestad de adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación, supervisión y fiscalización que le competen, y el inciso l) establece la potestad de la Superintendencia para requerir a los supervisados toda la información razonablemente necesaria a fin de cumplir la función supervisora del mercado de valores.

V. El artículo 38, literal f) del Régimen Privado de Pensiones, Ley 7523, establece como una atribución del superintendente de Pensiones adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación, supervisión y fiscalización que le competen a la Superintendencia, según la ley y las normas emitidas por el Conassif.

VI. Que el artículo 29 de la Ley Reguladora del Mercado de Seguros, Ley 8653, establece como objeto de la Sugese, velar por la estabilidad y el eficiente funcionamiento del mercado de seguros, así como entregar la más amplia información a los asegurados. La misma ley autoriza a la Sugese para regular y supervisar a las personas que intervengan en los actos o contratos relacionados con la actividad aseguradora, reaseguradora, la oferta pública y la realización de negocios de seguros. Asimismo, en el inciso i) del citado artículo se establece como su función el proponer al Conassif, para su aprobación, la normativa reglamentaria que se requiera para la aplicación de esta ley, así como cumplir sus competencias y funciones.

VII. El inciso n) y el sub inciso xi) del artículo 131 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558; el inciso r) del el artículo 38 de la Ley de Régimen Privado de Pensiones, Ley 7523; el inciso L) del artículo 8 de la Ley Reguladora del Mercado de Valores, y los incisos i) y j) del artículo 29 de la Ley Reguladora del Mercado de Valores, Ley 8653, facultan por su orden a la Superintendencia General de Entidades Financieras, a la Superintendencia de Pensiones, a la Superintendencia General de Valores y a la Superintendencia General de Seguros, a proponer al Conassif normas sobre el contenido, la forma y la periodicidad con que las entidades deben proporcionar a la Superintendencia, información sobre su situación jurídica, económica, financiera, de gobierno corporativo y de administración de riesgos, entre otros, para cumplir la supervisión que debe realizar cada una de las Superintendencias.

VIII. El inciso e) del artículo 131 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558; el artículo 40 de la Ley de Régimen Privado de Pensiones, Ley 7523; el inciso j) del artículo 8 de la Ley Reguladora del Mercado de Valores, y, el párrafo segundo y el inciso l) del artículo 29 de la Ley Reguladora del Mercado de Seguros, Ley 8653, facultan por su orden a la Superintendencia General de Entidades Financieras, a la Superintendencia de Pensiones, a la Superintendencia General de Valores y a la Superintendencia General de Seguros, a dictar medidas correctivas.

IX. Mediante artículo 13 del acta de la sesión 893-2010, celebrada el 3 de diciembre del 2010, el Conassif aprobó el Reglamento General de Auditores Externos, Acuerdo CONASSIF 1-10, el cual regula la contratación y la prestación de los servicios de auditoría externa.

X. Mediante artículos 5 y 7, de las actas de las sesiones 1294-2016 y 1295-2016, celebradas el 8 de noviembre de 2016, el Conassif aprobó el Reglamento sobre Gobierno Corporativo, Acuerdo CONASSIF 4-16 (anteriormente conocido como Acuerdo SUGEF 16-16), mediante el cual se establecen los principios sobre gobierno corporativo que deben considerar las entidades incluidas en el alcance de ese reglamento.

XI. Mediante artículos 9 y 11 de las actas de las sesiones 1318-2017 y 1319-2017, celebradas el 13 y el 20 de marzo del 2017, respectivamente, el Conassif aprobó el Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17 (anteriormente conocido como Acuerdo Sugef 14-17), el cual establece los requerimientos mínimos para la gestión de la tecnología de información (TI) que deben acatar las entidades y empresas supervisadas del sistema financiero costarricense incluidas en el alcance de ese reglamento.

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

XII. El Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17, requiere ser modificado integralmente con el fin de alcanzar los siguientes propósitos:

a. Reforzar las funciones de los Órganos de Dirección, Alta Gerencia y Órganos de Control con relación al marco de gobierno y de gestión de TI, incluyendo responsabilidades sobre la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital.

b. Actualizar el marco de gobierno y de gestión de TI e incorporar disposiciones sobre tecnologías emergentes, gobierno y gestión de la seguridad de la información, seguridad cibernética, incidentes de seguridad de la información, incidentes de seguridad cibernética, tercerización de bienes y servicios de TI, computación en la nube, el tratamiento del uso y acceso de los datos y de los activos de información.

consideraciones sobre el gobierno de la tecnología de información

XIII. El gobierno de la tecnología de información es una parte fundamental del gobierno corporativo y debe ser ejercido por el Órgano de Dirección, el cual, debe supervisar la definición e implementación de procesos, estructuras y mecanismos relacionados con TI. Lo anterior, con el fin de controlar eficazmente los procesos, garantizar la seguridad de la información, optimizar el uso de recursos y dar apoyo para la toma de decisiones; esto alineado con la visión, misión y objetivos estratégicos de la organización.

XIV. Se espera que los miembros de los Órganos de Dirección y de la Alta Gerencia se comprometan a adaptar e implementar sus medidas de gobierno conforme a su contexto, necesidades específicas y riesgos.

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

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

consideraciones sobre la gestión de la tecnología de información

XVI. Si bien la tecnología de información es indispensable para mantener y optimizar las operaciones dentro de las organizaciones, también su uso ha ocasionado la aparición de nuevos riesgos, por lo que es importante que el marco de gobierno y de gestión de TI incluya medidas sólidas para mitigar los riesgos que genera la dependencia tecnológica de las entidades y empresas supervisadas, y así garantizar su continuidad operativa en caso de incidentes tecnológicos.

XVII. El diseño e implementación del marco de gestión de TI requiere de esfuerzo planificado y progresivo. Además, requiere que se considere el entendimiento de la estrategia y su contexto organizacional, la determinación del alcance y la aplicabilidad de los componentes a implementar, así como sus factores de diseño, perfilamiento del alcance, el diseño de los procesos de negocio y la dependencia tecnológica de sus actividades.

consideraciones prudenciales sobre la seguridad de los servicios en la nube

XVIII. La migración a la nube brinda enormes oportunidades, eficiencia y conveniencia. Sin embargo, también expone a las organizaciones a una nueva gama de amenazas de seguridad de la información y seguridad cibernética, ya que se deben considerar las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube. Lo anterior, en función del tipo de modelo de implementación y el tipo de servicio de computación en la nube adquirido.

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

los modelos de implementación y los tipos de servicios de computación en la nube, así como los controles administrativos y técnicos asociados a este tipo de servicios.

consideraciones prudenciales sobre la tercerización de bienes y servicios de TI

XX. Los proveedores de bienes y servicios son ampliamente utilizados para proporcionar servicios, sistemas y soluciones de TI que respaldan las operaciones de las organizaciones. Las vulnerabilidades de la seguridad de la información, así como de la seguridad cibernética producto de la tercerización de bienes y servicios de TI podrían convertirse en canales de ciberataques, por lo que las capacidades de seguridad de la información y seguridad cibernética de los proveedores son elementos críticos.

XXI. Los proveedores de bienes y servicios de TI y su cadena de suministro no están dentro del alcance de esta regulación. Sin embargo, es necesario que las entidades y empresas supervisadas asuman su responsabilidad en el gobierno y la gestión de la seguridad de la información y la seguridad cibernética de aquellos bienes y servicios de TI tercerizados; lo anterior, 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.

XXII. Los más reconocidos proveedores internacionales de servicios en la nube, servicios de cómputo, almacenamiento, bases de datos, análisis e inteligencia artificial se encuentran a la vanguardia en el uso de herramientas e implementación de políticas de seguridad de la información y seguridad cibernética. Sin embargo, sus servicios suelen contratarse mediante instrumentos de adhesión; lo que hace necesario establecer un tratamiento diferenciado en la aplicación de la regulación, de manera que el marco regulatorio no impida la contratación de servicios con esos proveedores ni la supervisión por parte de las Superintendencias. En los casos en que los servicios se contraten mediante instrumentos de adhesión, la entidad debe ser responsable de asegurar la confidencialidad y la continuidad de los bienes y servicios delegados.

consideraciones sobre la seguridad de la información y la seguridad cibernética

XXIII. Los riesgos que amenazan la seguridad de la información y la seguridad cibernética han tomado importancia en un entorno creciente de conectividad y de dependencia de los servicios otorgados a través de plataformas tecnológicas, lo que conlleva a que las organizaciones, por una parte, deban asegurar la adecuada calidad y disponibilidad de los sistemas utilizados para la prestación de dichos servicios y , por otra parte, enfrenten una progresiva exposición a los riesgos, especialmente cuando estos se asumen en el ciberespacio.

XXIV. Los ciberataques sufridos por entidades financieras han centrado la atención en la necesidad de reforzar la seguridad cibernética. El Consejo de Estabilidad Financiera (FSB por sus siglas en inglés) incluyó en su plan de trabajo de 2017, la necesidad de vigilar el riesgo cibernético derivado de la tecnología financiera e identificar los asuntos de supervisión y regulación desde la perspectiva de la estabilidad financiera.

XXV. En junio de 2016, el Comité de Pagos e Infraestructuras de Mercado (CPMI) y la Organización Internacional de Comisiones de Valores (IOSCO) publicaron orientaciones sobre la ciberresistencia de las infraestructuras de los mercados financieros. Además, en abril de 2016, la Asociación Internacional de Supervisores de Seguros (IAIS) publicó un documento temático para sensibilizar a las aseguradoras y a los supervisores sobre los retos que plantea el riesgo cibernético.

XXVI. El Comité de Supervisión Bancaria de Basilea reconoció los beneficios de abordar la resiliencia operacional más allá del ámbito de la gestión del riesgo operacional y los requerimientos de capital mínimos. A principios de 2018, estableció el grupo de trabajo de resiliencia operacional (ORG) con la intención de contribuir, entre otros aspectos, a los esfuerzos internacionales relacionados con la gestión del riesgo cibernético.

XXVII. Es importante que las entidades y empresas supervisadas cuenten con un marco regulatorio que contemple las buenas prácticas en materia de seguridad de la información y seguridad cibernética, lo que deriva en mejoras para contar con una adecuada gestión de su negocio, así como anticiparse a posibles escenarios adversos. El presente reglamento otorgará claridad a las entidades y entidades supervisadas sobre los elementos mínimos de seguridad de la información y seguridad cibernética que resultan esenciales para el regulador, así como la notificación oportuna de incidentes, sus impactos y su gestión.

XXVIII. Se espera que las entidades y empresas supervisadas establezcan un Sistema de Gestión de Seguridad de la Información a través de la definición de estructuras generales para el gobierno y gestión, de conformidad con lo establecido en el marco de gestión de TI del presente reglamento.

consideraciones prudenciales sobre la auditoría externa de TI

XXIX. El proceso de supervisión de TI se apoya en auditorías externas especializadas, cuyos alcances son definidos por el supervisor a partir de un conjunto de procesos de evaluación relacionados con el marco de gobierno y de gestión de TI, en congruencia con el perfil tecnológico comunicado por las entidades y empresas supervisadas.

XXX. La auditoría de TI es una actividad especializada para la cual existen certificaciones con reconocimiento mundial. En el caso de la certificación Certified Information Systems Auditor (CISA por sus siglas en inglés) emitida por ISACA, esta reconoce las aptitudes y conocimientos de un profesional en las áreas de auditoría de sistemas de información, gobierno y mantenimiento de TI, adquisición, desarrollo e implementación de sistemas de información, operaciones, mantenimiento y soporte de sistemas de información y protección de activos de información.

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

XXXI. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) de Costa Rica estableció una Estrategia Nacional de Ciberseguridad con el objetivo de diseñar un marco para orientar las acciones que el país puede tomar con respecto al uso seguro de TI y desarrollar la coordinación y cooperación entre las partes interesadas. El papel del regulador incluye contar con un marco normativo basado en buenas prácticas para la protección de infraestructuras críticas con el fin de desarrollar una infraestructura de monitoreo y alerta temprana para la detección, prevención y respuesta de incidentes de seguridad cibernética.

XXXII. Las asociaciones profesionales, entidades globales, gobiernos de diferentes jurisdicciones, así como diferentes industrias y los profesionales en TI, han desarrollado estándares, buenas prácticas y marcos de referencia para gestionar y controlar las tecnologías y sus riesgos relacionados, los cuales han sido considerados en las disposiciones del presente reglamento y estos, a su vez, se alinean con el objetivo de la Estrategia Nacional de Ciberseguridad establecida por el Micitt.

XXXIII. El marco de referencia COBIT 2019, emitido por ISACA, permite la alineación, interoperabilidad e integración con los estándares, buenas prácticas y otros marcos de referencia desarrollados por la industria y los profesionales de TI, lo cual, permite fortalecer el control interno de las tecnologías de información.

XXXIV. En la industria de TI, se identifican un conjunto de marcos de referencia y estándares en materia de seguridad cibernética, como el caso de los estándares desarrollados por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés), que se enfocan en el uso de impulsores de negocios para guiar las actividades de seguridad cibernética y en la consideración de los riesgos de seguridad cibernética. Asimismo, se desarrollaron las normas ISO que disponen de estándares orientados en materia de seguridad cibernética, los Controles CIS del Center for Internet Security y los controles del Cloud Security Alliance.

XXXV. La regulación permite que las entidades y empresas supervisadas utilicen los estándares internacionales, mejores prácticas y marcos de referencia que la industria

de tecnologías ha desarrollado para la implementación del marco de gobierno y de gestión de TI, sin perjuicio del cumplimiento de las disposiciones establecidas en este reglamento.

consideraciones de costo-beneficio

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

otras consideraciones

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

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

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

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

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

No obstante, en dicho criterio se reconoce que:

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

Ahora bien, la Procuraduría concluye que:

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

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

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

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

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

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

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

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

Finalmente, y por tratarse de una norma transversal, resulta indispensable que la modificación propuesta se apruebe no solo para los regulados por la Sugef, la Sugeval y la Sugese; este cambio debe ser aprobado también para los regulados por la Supen con el propósito de asegurar un trato uniforme con el resto de las empresas y entidades supervisadas de los grupos y conglomerados financieros y para evitar

los espacios de asimetría regulatoria, que se podrían generar como consecuencia de la aplicación de una regulación desigual entre las entidades supervisadas del sistema financiero, sin que exista una justificación técnica para ello.

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

"Esta Sala ha aceptado válidamente, la aplicación de la teoría del funcionario de hecho, estipulada en la Ley General de la Administración Pública, en sus artículos 155 y siguientes. En reiteradas ocasiones, (vid sentencias N.° 2765-92, 15:30 horas del 01-09-92 y N.° 6701-93, 15:06 del 21-12-93) ha manifestado que las actuaciones realizadas por un funcionario de hecho, revisten su carácter de validez en tanto se cumplan determinados requisitos o condiciones, **ello con la necesidad de preservar el interés general, mismo que constituye el principal objetivo que ha de ser atendido por el ordenamiento jurídico**. Por lo que acerca de los requisitos para reconocer la validez de los actos de los funcionarios de hecho, se encuentra este tribunal los siguientes:

´ ... Que exteriormente se presenten como si emanaran de funcionarios de jure, es decir, deben producir, respectos a terceros, al público, los efectos jurídicos propios de los actos que emanan de agentes verdaderamente regulares... **El reconocimiento de la validez de esos actos en favor de los terceros, debe ser "de interés público", en busca de la seguridad jurídica y la certidumbre del derecho**... También es necesario que lo actuado por el funcionario de hecho se haya realizado dentro de los límites de competencia de la autoridad oficial que dicho funcionario pretende tener...´ (Sentencia número 6701-93)". [Lo resaltado no es del original].

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

"El carácter de interés público de la regulación financiera es indiscutible y se origina en el hecho mismo, repetimos, que las entidades financieras actúan en el mercado, captando, manejando, invirtiendo el ahorro **de terceros. De allí la necesidad de regular que las entidades no incurran en riesgos que lesionan el interés de los ahorrantes o inversionistas.**

Por ese poder de policía de contenido financiero, se permite a los órganos regulador y supervisor reglamentar la actividad financiera y los agentes que en ella intervienen, dictando normas que permiten interpretar e integrar las leyes en la materia, vigilar el funcionamiento del sistema y aplicar esas leyes; en su caso, sancionar el irrespeto al régimen especial. De esa forma, se orienta y dirige la

actividad financiera necesaria para atender las necesidades de la producción y el consumo, así como satisfacer los intereses de los inversionistas o ahorrantes. Importa destacar que se reconoce la posibilidad de imponer reglas de comportamiento a los intermediarios financieros, tendientes a prevenir que incurran en riesgos excesivos y a garantizar la solvencia y la liquidez de los establecimientos. El objetivo último: la estabilidad y solvencia de los distintos agentes financieros y del sistema en general". Dictamen N. C-320-2005 de 6 de setiembre de 2005.

A la estabilidad y solvencia de los entes supervisados por la Superintendencia de Pensiones, **se une la finalidad social propia del régimen de pensiones**, que no es otra que la protección del trabajador y ex trabajador en caso de invalidez, vejez y muerte. […]" [Lo resaltado no es del original].

XXXIX. Mediante artículos 4 y 5 de las actas de las sesiones 1834-2023 y 1835-2023, celebradas el 20 de noviembre del 2023, el Conassif remitió a consulta pública la propuesta de modificación al Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17, en el entendido que, en un plazo máximo de quince días hábiles, contados a partir del día hábil siguiente del recibo de la respectiva comunicación, las entidades del Sistema Financiero Nacional podían enviar al Despacho de la superintendente general de entidades financieras sus comentarios y observaciones. Posteriormente, mediante artículos 6 y 4 de las actas de las sesiones 1837-2023 y 1838-2023, celebradas el 4 y 6 de diciembre del 2023, el Conassif dispuso extender, al 15 de enero del 2024, el plazo para la recepción de comentarios y observaciones a la citada propuesta de modificación normativa remitida en consulta. No obstante, debido a los cambios y mejoras incorporados en la propuesta de modificación reglamentaria a partir de los resultados del proceso de consulta, el Consejo consideró conveniente enviarla nuevamente en consulta al medio, por lo que, mediante artículos 6 y 5 de las actas de las sesiones 1853-2024 y 1854-2024, celebradas el 16 de abril del 2024, el Conassif dispuso el envío en consulta de la citada propuesta de modificación reglamentaria en una segunda instancia durante un plazo de diez días hábiles; se recibieron comentarios y observaciones, los cuales, fueron evaluados y en lo pertinente fueron incorporadas al texto de la modificación reglamentaria.

dispuso por mayoría y en firme:

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:

CONASSIF
Consejo Nacional de Supervisión del Sistema Financiero

REGLAMENTO GENERAL DE GOBIERNO Y GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

ACUERDO CONASSIF 5-24

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

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

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

Artículo 2. Alcance

Las disposiciones establecidas en este reglamento son de aplicación para:

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

b) Supervisados por SUGEVAL:
- **1.** Puestos de bolsa y sociedades administradoras de fondos de inversión
- **2.** Bolsas de valores
- **3.** Sociedades de compensación y liquidación
- **4.** Proveedores de precio
- **5.** Entidades que brindan servicios de custodia
- **6.** Centrales de valores
- **7.** Sociedades titularizadoras y fiduciarias

8. Entidades de registros centralizados de letras de cambio y pagarés electrónicos

c) Supervisados por SUGESE:
1. Entidades aseguradoras y reaseguradoras
2. Sucursales de entidades aseguradoras extranjeras
3. Sociedades corredoras de seguros

d) Supervisados por SUPEN:
1. Operadoras de pensiones complementarias
2. Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social
3. Fondos complementarios creados por leyes especiales o convenciones colectivas

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

Se exceptúan del alcance del presente reglamento a los regímenes administrados por la Dirección Nacional de Pensiones del Ministerio de Trabajo, las entidades reguladas y fondos en proceso de liquidación, los fondos creados por leyes especiales que son administrados por una operadora de pensiones o en los casos en que la unidad de TI y su gestión de TI es regulada por una norma de tecnología de información de alcance general, cuyo cumplimiento esté debidamente fiscalizado, así como los fondos de pensiones cerrados a nuevas afiliaciones.

e) Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados.

Artículo 3. Regulación Proporcional

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

1. Lo dispuesto en los capítulos que se indican a continuación se considerará como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades en función de sus riesgos, tamaño, complejidad y modelo de negocio: a) Capítulo II Gobierno y Gestión de TI, b) Capítulo III Organización de las tecnologías de información.

2. Lo dispuesto en el Capítulo IV Seguridad de la información y seguridad cibernética, será de aplicación plena, salvo en el caso de lo dispuesto en: a) El artículo 33. Programas de análisis de vulnerabilidades y pruebas, b) El artículo 34. Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión de riesgos de

seguridad cibernética y en c) El artículo 35. Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética, del presente reglamento.

Los artículos 33, 34 y 35 se consideran como referencias sobre sanas prácticas que las entidades, discrecionalmente, podrán adoptar en función de sus riesgos, tamaño, complejidad y modelo de negocio.

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

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

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

b) Sin perjuicio de lo anterior, el alcance de la auditoría externa deberá incluir, al menos, los procesos de evaluación que se especifican en el anexo 2 de los lineamientos generales del presente reglamento.

Artículo 4. Definiciones y abreviaturas

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

a) **Activos digitales**: Todo tipo de datos o activos de información que se presenten en formato digital, los cuales, sean propiedad de una entidad o empresa supervisada o de sus partes interesadas y que permiten a estas mantener sus operaciones digitales y tecnológicas.

b) **Bienes y servicios de TI críticos**: Son aquellos productos, servicios o recursos que son esenciales para el funcionamiento continuo y efectivo de una entidad o empresa supervisada, cuya interrupción o falta podría tener un impacto significativo en sus operaciones, objetivos, reputación o el ecosistema financiero.

c) **Declaración de aplicabilidad**: Documento que permite identificar y revelar los controles de seguridad de la información y de la seguridad cibernética elegidos por la entidad o empresa supervisada para proteger sus activos de información, basándose en la evaluación de riesgos.

d) **Gestión de TI**: Conjunto de estructura de relaciones y procesos para planificar, construir, ejecutar y monitorear la tecnología de la información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.

e) **Gobierno de TI**: Subcomponente del gobierno corporativo, el cual, se encarga de la evaluación, dirección y supervisión de las tecnologías de información.

f) **ISACA**: Acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association).

g) **Marco de gobierno y gestión de TI**: Conjunto de procesos destinados a gobernar y gestionar las tecnologías de información de las entidades y empresas supervisadas, los cuales, deben ser adoptados y adaptados para gobernar y gestionar de forma integral los riesgos relacionados con las tecnologías e información, considerando su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica que estas tienen en los procesos de TI.

h) **Perfil tecnológico**: Descripción de la estructura de gobierno y gestión, los procesos, servicios, infraestructura de TI, proveedores de bienes y servicios de TI, inventario de tipos documentales, proyectos de TI, planes de adquisición y gestión de riesgos de TI.

i) **Plan de acción**: Conjunto de acciones, plazos y responsables enfocados en atender los hallazgos y riesgos detectados en el informe de auditoría y comunicados en el reporte de supervisión.

j) **Procesos críticos**: Son aquellos procesos que tienen un impacto significativo en la consecución de los objetivos estratégicos previstos por la entidad o empresa supervisada. Estos procesos están relacionados con la naturaleza, misión, objetivos y función de la entidad o empresa supervisada y son indispensables para la continuidad del negocio y de sus operaciones.

k) **Proveedores de bienes y servicios de TI críticos**: Persona física o jurídica que provee bienes o servicios de TI a la entidad o empresa supervisada, los cuales, apoyan los procesos críticos indistintamente de su domicilio, incluyendo subcontratistas o partners (asociados).

l) **Resiliencia operativa digital**: Capacidad de una entidad o empresa supervisada para mantener la continuidad y la disponibilidad de sus operaciones digitales y tecnológicas incluso en situaciones adversas. Implica la implementación de medidas proactivas y estrategias para garantizar que las operaciones digitales sigan funcionando de manera eficiente y segura, minimizando el impacto de los incidentes.

m) **Seguridad cibernética**: Práctica de gestionar los riesgos para proteger sistemas, redes, dispositivos y datos digitales contra amenazas, ataques y actividades maliciosas en el ciberespacio, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información y de los recursos digitales.

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

o) **Tecnología de información (TI)**: Conjunto de técnicas para la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos de negocios, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad, entre otros.

p) **Unidad de TI o función equivalente**: Instancia o función que provee los procesos y ervicios de TI para las entidades y empresas supervisadas.

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

Artículo 5. Lineamientos generales

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

CAPÍTULO II

GOBIERNO Y GESTIÓN DE TI

Sección I. Marco de gobierno y gestión de TI

Artículo 6. Marco de gobierno y gestión de TI

Las entidades y empresas supervisadas deben diseñar, implementar, controlar y mantener un marco de gobierno y gestión de TI de conformidad con: la estrategia organizacional; el apetito, la tolerancia y la capacidad de riesgo; el tamaño, complejidad, modelo de negocio y las políticas aprobadas por el Órgano de Dirección.

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

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

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

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

a) Orientar hacia la definición del gobierno de TI con un enfoque integrado y alineado con el gobierno corporativo.

b) Asegurar un equilibrio entre el uso de los recursos de TI, servicios de TI y los procesos críticos de negocio.

c) Crear valor mediante los beneficios de las tecnologías de información, dentro de los márgenes de apetito, tolerancia y capacidad de riesgo.

d) Asegurar que la entidad o empresa supervisada dispone de recursos adecuados y suficientes para el gobierno y la gestión de TI.

e) Asegurar que se identifica e involucra a las partes interesadas en el diseño del marco de gobierno y gestión de TI.

f) Diseñar e implementar el marco de gobierno y gestión de TI de conformidad con los objetivos y riesgos del negocio.

g) Asegurar que la planificación estratégica de TI permita una visión holística de la entidad o empresa supervisada en su entorno actual, así como de su dirección futura.

h) Establecer una dirección y una estructura eficiente para gestionar TI; además, alinear los objetivos de la entidad o empresa supervisada con el uso de la tecnología y su arquitectura organizacional.

i) Gestionar la innovación, las tecnologías emergentes, el conocimiento y los datos relacionados con la entidad o empresa supervisada.

j) Gestionar el presupuesto, los costos, el conocimiento y el recurso humano de la unidad de TI, así como las relaciones con las partes interesadas.

k) Establecer la gestión de los acuerdos de nivel de servicio, de los proveedores de bienes y servicios de TI, así como la gestión de los riesgos de TI de manera holística en la entidad o empresa supervisada.

l) Establecer el diseño e implementación de sistemas integrados de calidad y de seguridad de la información, así como la gestión de activos de información y de los datos.

m) Definir la gestión del portafolio, de los programas y de los proyectos de TI que permitan atender la definición de los requisitos del negocio.

n) Determinar la estrategia de adquisición, construcción e implementación de soluciones tecnológicas integradas al negocio.

o) Gestionar la disponibilidad y la capacidad de infraestructura tecnológica, así como asegurar la continuidad de las operaciones.

p) Asegurar la configuración y la seguridad de los activos de información, así como asegurar la información que dichos activos soportan, de conformidad con la gestión, aceptación y transición de los cambios.

q) Gestionar las operaciones de TI, los incidentes, la solución de los problemas de TI, los servicios de seguridad de la información y de seguridad cibernética, así como los controles de los procesos del negocio; además, asegurar una resiliencia operativa digital.

r) Gestionar el monitoreo del desempeño y la conformidad de los procesos, del sistema de control interno, del cumplimiento de los requisitos externos, así como del cumplimiento normativo, la legislación nacional aplicable y del aseguramiento de TI.

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

Sección II. Responsabilidades del Órgano de Dirección

Artículo 8. Responsabilidades generales sobre el gobierno de TI

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

a) Aprobar el marco de gobierno y gestión de TI, así como asegurar que la declaración de apetito de riesgo incorpore el apetito, la tolerancia y la capacidad de los riesgos asociados a TI.

b) Establecer un Comité de TI o una función equivalente y aprobar sus normas de gobierno y gestión.

c) Aprobar las políticas, estructuras, estrategias, recursos, inversiones y presupuestos necesarios para la implementación del marco de gobierno y gestión de TI, así como para las tecnologías emergentes que se implementen.

d) Aprobar los informes de la auditoría externa de TI que serán remitidos a las Superintendencias.

e) Aprobar los planes de acción para la atención de los hallazgos y de los riesgos que se identifiquen como resultado de la auditoría externa de TI.

f) Asegurar que se consideren las necesidades de las partes interesadas para lograr un equilibrio entre los objetivos del negocio y los objetivos de TI definidos por la entidad o empresa supervisada.

g) Designar las áreas de negocio y de TI responsables de diseñar e implementar el marco de gobierno y de gestión TI.

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

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

a) Asegurar que la gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética estén integrados dentro de la gestión de riesgos de la entidad o empresa supervisada.

b) Promover las discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética en las reuniones del Órgano de Dirección.

c) Asegurar el establecimiento de un sistema de gestión de la seguridad de la información, así como sus controles.

d) Aprobar los planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética.

Artículo 10. Responsabilidades sobre la resiliencia operativa digital

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

a) Aprobar las políticas de resiliencia operativa digital de la entidad o empresa supervisada.

b) Asegurar que la resiliencia operativa digital esté incorporada dentro de los planes de contingencia y continuidad de negocio.

c) Aprobar los presupuestos y recursos necesarios para asegurar la resiliencia operativa digital.

d) Asegurar que se implementen planes de respuesta, recuperación y atención de crisis para gestionar los incidentes relacionados con los activos digitales que podrían interrumpir la ejecución de los procesos críticos.

e) Asegurar que los planes de respuesta de incidentes relacionados con los activos digitales sean acordes con el apetito, tolerancia y capacidad de riesgo establecidos por la entidad o empresa supervisada.

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

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

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

a) Implementar el marco de gobierno y gestión de TI aprobado por el Órgano de Dirección.

b) Proponer al Órgano de Dirección la estrategia y los recursos requeridos para la implementación del marco de gobierno y gestión de TI.

c) Implementar las políticas relacionadas con TI aprobadas por el Órgano de Dirección.

d) Implementar los planes de acción para la atención de los hallazgos de la auditoría externa de TI.

e) Asegurar que se resguarde la confidencialidad e integridad de los datos y de la información crítica de las partes interesadas y de la entidad o empresa supervisada que sea utilizada, almacenada o procesada por terceros.

f) Asegurar que se establezcan las medidas para la gestión de los incidentes de seguridad de la información y seguridad cibernética.

g) Asegurar que los requerimientos de seguridad de la información y de seguridad cibernética de la entidad o empresa supervisada sean de cumplimiento por parte de sus proveedores de bienes y servicios de TI.

h) Asegurar que la gestión de los datos de la entidad o empresa supervisada se realice de manera efectiva y eficiente; asimismo, que las necesidades de confidencialidad, integridad, disponibilidad, no repudio y auditabilidad, sean atendidas, en función de sus riesgos.

Artículo 12. Comité de TI o función equivalente

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

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

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

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

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

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

a) Supervisar la implementación del marco de gobierno y gestión de TI.

b) Asesorar al Órgano de Dirección y a la Alta Gerencia en la formulación de las estrategias y las metas de TI; asimismo, velar por su cumplimiento.

c) Proponer al Órgano de Dirección las políticas relacionadas con TI.

d) Proponer al Órgano de Dirección los planes de acción que, cuando corresponda, atenderán las observaciones incluidas en el reporte de supervisión de TI, así como monitorear su implementación.

e) Validar que los procedimientos, los instructivos y la documentación de TI sean implementados desde las unidades funcionales responsables de ejecutarlos.

f) Recomendar al Órgano de Dirección las prioridades para las inversiones en TI.

g) Validar que la firma de auditores externos o el profesional independiente de TI tengan los conocimientos y la experiencia para auditar aspectos de seguridad de la información, seguridad cibernética, tecnologías emergentes u otros aspectos, de conformidad con el alcance solicitado.

h) Validar el estudio técnico en el que se fundamentan los procesos de evaluación del marco de gobierno y gestión de TI que no le aplican a la entidad o empresa supervisada.

Sección IV. Responsabilidades de los Órganos de Control

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

En relación con las tecnologías de información, la Auditoría Interna o la función equivalente, como parte de la planificación de los estudios de la auditoría interna y su universo auditable, al menos, debe:

a) Verificar 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, el cual, permita evaluar la calidad y la eficacia del marco de gobierno y gestión de TI, de la seguridad de la información y de la seguridad cibernética.

c) Evaluar la calidad y eficacia de los planes de acción elaborados por la entidad o empresa supervisada que atenderán los hallazgos que se identifiquen como resultado de la auditoría externa de TI.

d) Ejecutar trabajos específicos requeridos por las Superintendencias.

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

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

a) Incorporar la gestión de los riesgos tecnológicos, de tecnologías emergentes, de la seguridad de la información y de la seguridad cibernética dentro de la gestión de riesgos de la entidad o empresa supervisada.

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

c) Ejecutar trabajos específicos requeridos por las Superintendencias.

CAPÍTULO III

ORGANIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

Sección I. Generalidades de la gestión de TI

Artículo 16. Gestión de TI individual o función corporativa

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

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

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

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

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

Artículo 17. Unidad de TI o función equivalente

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

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

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

a) Ejecutar las estrategias para la implementación del marco de gobierno y gestión de TI.

b) Implementar los proyectos relacionados con TI de acuerdo con el plazo, el presupuesto y los requisitos establecidos.

c) Diseñar e implementar la arquitectura tecnológica, la arquitectura de información y de aplicaciones, alineadas a la arquitectura de negocio, a fin de soportar las operaciones de la entidad o empresa supervisada.

d) Establecer los controles para el desarrollo del ciclo de vida de los servicios, de las aplicaciones, de los sistemas de información y de las soluciones tecnológicas, los cuales, aseguren la confidencialidad, integridad, disponibilidad, calidad, mantenimiento y los cambios por excepción o de emergencia.

e) Asegurar que los bienes y servicios de TI críticos estén identificados; además, asegurar que se mantengan disponibles y que sean gestionados de manera efectiva y eficiente.

f) Asegurar que los requerimientos de las entidades y empresas supervisadas sean atendidos de manera equitativa y en función de los riesgos de cada entidad o empresa que constituye el grupo o conglomerado cuando la gestión de TI sea tipificada como corporativa.

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

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

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

Las entidades y empresas supervisadas deben etiquetar los activos de información según su nivel de confidencialidad, de conformidad con el modelo de clasificación de acceso y uso de

los activos de información y datos establecido en los lineamientos generales del presente reglamento.

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

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

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

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

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

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

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

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

Sección III. Gestión de la computación en la nube

Artículo 22. Servicios de computación en la nube

Las entidades y empresas supervisadas pueden disponer de sus componentes tecnológicos mediante el uso de servicios de computación en la nube, siempre y cuando, cumplan con las

obligaciones generales para uso de la computación en la nube establecidas en el presente reglamento.

Cuando las entidades y empresas supervisadas deleguen sus procesos críticos a través de servicios de computación en la nube, deben establecer las obligaciones de cada una de las partes involucradas para proteger los datos, el software, la plataforma y la infraestructura en la nube.

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

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

a) Gestionar los riesgos derivados del uso de servicios de computación en la nube.

b) Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube. Dichos criterios deben considerar, al menos, la seguridad, fiabilidad, escalabilidad, costo, soporte, experiencia, interoperabilidad y cumplimiento regulatorio.

c) Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001. Además, de conformidad con el servicio externalizado, verificar que cumpla con estándares o buenas prácticas, tales como las ISO 27017, 27018 o las mejores prácticas del Cloud Security Alliance.

d) Asegurar que los niveles de disponibilidad estén de conformidad con los objetivos de resiliencia (RPO y RTO) establecidos por la entidad o empresa supervisada.

e) Establecer controles para asegurar la disponibilidad acordada del servicio con el proveedor.

f) Establecer mecanismos que permitan contar con respaldo de la información que se procesa y almacena en la nube, la cual, debe estar a disposición de la entidad o empresa supervisada en un sitio alterno que asegure la confidencialidad, integridad y disponibilidad de la información. Lo anterior, cuando los servicios contratados, por su naturaleza, no garanticen o incluyan el respaldo.

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

h) Tener bajo su control la administración de usuarios y privilegios para el acceso a los servicios de computación en la nube, a las plataformas, las aplicaciones y las bases de datos que operen en la nube. Lo anterior, de conformidad con el modelo de servicio contratado.

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

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

k) Monitorear el cumplimiento de los acuerdos de niveles de servicio establecidos con el proveedor de servicios en la nube y, en caso de que aplique, de sus subcontratistas.

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

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

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

Sección IV. Tercerización de bienes y servicios de TI

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

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

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

Las entidades y empresas supervisadas deben establecer controles a fin de comprobar que los proveedores que les suministran bienes y servicios de TI implementan medidas para gestionar la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital, de conformidad con los requerimientos definidos por las entidades y empresas supervisadas.

Cuando los bienes y servicios de TI críticos sean proveídos por terceros, las entidades y empresas supervisadas deben asegurar que, en caso de que dichos bienes y servicios, a su vez, sean subcontratados por los terceros, se cuente con controles de seguridad de la información y seguridad cibernética, asimismo, que se cuente con planes de continuidad del negocio.

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

Artículo 26. Identificación de la información y de los bienes y servicios de TI proveídos por terceros

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

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

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

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

Artículo 28. Acuerdos de confidencialidad

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

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

Artículo 29. Contratos y acuerdos de nivel de servicio

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

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

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

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

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

Artículo 30. Acceso de las Superintendencias a la información

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

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

CAPÍTULO IV

SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD CIBERNÉTICA

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

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

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

El sistema de gestión de la seguridad de la información debe establecer los controles que permitan adoptar un enfoque basado en el riesgo, para proteger los activos de información y los

activos que soportan la información, contra los riesgos de la seguridad de la información y de la seguridad cibernética. Los controles deberán ser incluidos en una declaración de aplicabilidad y especificar los atributos que están establecidos en los lineamientos generales del presente reglamento.

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

Las Superintendencias podrán requerir la inclusión de prácticas y controles de seguridad de la información y seguridad cibernética dentro del sistema de gestión de la seguridad de la información de acuerdo con los riesgos identificados.

Artículo 32. Seguridad cibernética

Las entidades y empresas supervisadas deben gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital.

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

Artículo 33. Programas de análisis de vulnerabilidades y pruebas

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

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

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

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

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

Las unidades, funciones organizacionales, centros de operaciones o comités técnicos deben establecerse de conformidad con la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por las entidades o empresas supervisadas.

Las unidades, funciones organizacionales, centros de operaciones o comités técnicos que gestionen los riesgos de seguridad cibernética pueden estar integrados a las áreas o funciones de seguridad de la información de las entidades o empresas supervisadas, tercerizadas o separadas.

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

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

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

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

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

Sección II. Incidentes de seguridad de la información y seguridad cibernética

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

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

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

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

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

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

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

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

a) Definir responsabilidades dentro de las áreas de gestión para facilitar su resolución y la coordinación entre todas las partes que la integran.

b) Establecer las directrices operativas e informativas durante la situación del incidente de seguridad de la información o de seguridad cibernética.

c) Evaluar las estrategias que se llevan a cabo, las acciones y los resultados.

d) Detectar y prever acontecimientos y pasos a seguir en función del desarrollo de los hechos para erradicar y resolver el incidente de seguridad de la información o de seguridad cibernética.

e) Identificar oportunidades de mejora para la gestión de incidentes de seguridad de la información y seguridad cibernética, así como implementar estrategias de mejora continua.

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

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

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

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

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

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

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

Artículo 40. Comunicado de incidentes a los clientes

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

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

Artículo 41. Información histórica de incidentes de seguridad de la información y seguridad cibernética

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

El contenido y el plazo de conservación de la información histórica está establecido en los lineamientos generales del presente reglamento.

CAPÍTULO V

LA AUDITORÍA EXTERNA DE TI

Sección I. Perfil tecnológico

Artículo 42. Perfil tecnológico

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

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

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

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

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

Las entidades y empresas supervisadas deben indicar en el perfil tecnológico cuáles de los procesos de evaluación detallados en el anexo 1 de los lineamientos generales del presente reglamento, resultan adecuados a su marco de gobierno y gestión de TI. Asimismo, las entidades y empresas supervisadas deberán indicar, en el perfil tecnológico, los procesos de evaluación que no les apliquen, así como los que estén externalizados de forma total o parcial.

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

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

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

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

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

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

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

Artículo 45. Comunicación de cambios significativos del perfil tecnológico

Las entidades y empresas supervisadas deben identificar los cambios que se realicen en el perfil tecnológico con respecto al perfil anterior, los cuales, consideren que son significativos en aspectos tales como impacto en: la operación, la seguridad, el cumplimiento, la inversión requerida, los beneficios esperados, el alcance de los procesos de evaluación aplicables a la entidad, los riesgos asociados y su alineación con la estrategia organizacional, entre otros. Lo anterior, en virtud de su naturaleza, tamaño, complejidad, modelo de negocio y riesgos.

Además, las entidades y empresas supervisadas deben comunicar dichos cambios significativos a las Superintendencias. El plazo y los canales de comunicación de los cambios significativos del perfil tecnológico están establecidos en los lineamientos generales del presente reglamento.

Sección II. Auditoría externa de TI

Artículo 46. Auditoría externa de TI

Las Superintendencias solicitarán a las entidades y empresas supervisadas la contratación de una auditoría externa de TI sobre el marco de gobierno y gestión de TI según el alcance determinado por el supervisor. Para las entidades sujetas a la aplicación del artículo 3.

Regulación proporcional, las Superintendencias solicitarán la contratación de una auditoría externa de TI de conformidad con lo establecido en dicho artículo.

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

Cuando las entidades y empresas supervisadas dispongan de sus componentes tecnológicos mediante el uso de servicios de computación en la nube proveídos por terceros o se celebren contratos de adhesión, 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 cuenten con auditorías independientes.

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

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

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

a) Los procesos de evaluación del marco de gobierno y gestión de TI establecidos en los anexos 1 y 2 de los lineamientos generales del presente reglamento, aplicables a la entidad en el momento de la solicitud de la auditoría externa de TI, de conformidad con los artículos 3 y 43 del presente reglamento.

b) Las funciones para la evaluación de la gestión de riesgos de seguridad cibernética establecidas en los lineamientos generales del presente reglamento.

c) Componentes revelados en el perfil tecnológico de la entidad o empresa supervisada.

d) Entidades y empresas supervisadas, así como áreas de negocio y áreas de TI por considerar en cada proceso.

e) Proveedores de bienes y servicios de TI que, según los riesgos identificados, requieran la evaluación de una auditoría externa de TI, en cuyo caso, se evaluaran los procesos aplicables a la entidad o empresa supervisada y cualquier otro aspecto que esté relacionado con los bienes y servicios de TI tercerizados.

f) El periodo de cobertura.

g) Aspectos que las Superintendencias requieran de conformidad con los riesgos identificados.

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

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

Artículo 48. Periodicidad de las auditorías externas de TI

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

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

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

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

b) la planificación del encargo.

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

Artículo 50. Productos de la auditoría externa de TI

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

a) El informe de la auditoría externa de TI.

b) La copia del acuerdo del Órgano de Dirección en el que se aprobó el informe de la auditoría externa de TI. Se debe indicar el número y fecha del acta en la que se consignó el acuerdo.

c) La matriz de evaluación del marco de gobierno y gestión de TI.

d) Cualquier otro producto solicitado por la Superintendencia en el alcance de la auditoría externa de TI.

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

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

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

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

Sección III. Reporte de supervisión y plan de acción

Artículo 52. Reporte de supervisión

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

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

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

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

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

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

El plazo dispuesto en el artículo 52 del presente reglamento para que las Superintendencias remitan el reporte de supervisión, iniciará nuevamente a partir de la última recepción de los productos corregidos.

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

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

Las entidades y empresas supervisadas deben elaborar un plan de acción para gestionar los hallazgos y los riesgos que se identifiquen como resultado de la auditoría externa de TI. Las acciones que se incluyan en el plan de acción deben establecerse en función del tamaño, complejidad y modelo de negocio, así como de los niveles de apetito, tolerancia y capacidad de riesgo establecidos.

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

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

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

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

Sección IV. Prórrogas

Artículo 55. Solicitudes de prórrogas

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

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

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

Artículo 56. Aceptación o rechazo de las solicitudes de prórrogas

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

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

DISPOSICIONES ADICIONALES

Disposición adicional primera. Referencias normativas

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

DISPOSICIONES TRANSITORIAS

Disposición transitoria primera. Auditorías externas de TI

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

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

Disposición transitoria segunda. Gestión de TI corporativa

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

Disposición transitoria tercera. Planes de acción vigentes

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

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

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

a) **Contratos nuevos**: A partir de la publicación de las modificaciones del presente reglamento en el diario oficial La Gaceta, deben acatarse las disposiciones sobre contratos y acuerdos de nivel de servicio.

b) **Contratos vigentes**: Continúan según lo acordado entre las partes. Las disposiciones aplicarán en caso de renovación del servicio y cuando deban suscribir nuevos contratos y acuerdos de nivel de servicio. En todo caso, las entidades y empresas supervisadas cuentan con un plazo no mayor a dieciocho meses a partir de la entrada en vigor del

presente reglamento para realizar los ajustes necesarios en los nuevos contratos y acuerdos de nivel de servicio.

En casos debidamente justificados, podrán otorgarse prórrogas de hasta seis meses.

Disposición transitoria quinta. Sociedades corredoras de seguros

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

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

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

b) En concordancia con la naturaleza, modelo de negocio, criticidad de los procesos y dependencia tecnológica de información y la complejidad de sus operaciones, la SUGESE requiere que las sociedades corredoras de seguros implementen su marco de gestión, así como los órganos, comités, instancias y controles, para lo cual deben contar con una estructura organizacional para la gestión de TI que delimite claramente sus obligaciones, funciones y responsabilidades y que cuente con políticas orientadas a cautelar una adecuada gestión de TI en congruencia con su estrategia de gestión de los riesgos de TI.

2. Perfil tecnológico de las sociedades corredoras de seguros:

a) Las sociedades corredoras de seguros remitirán su primer perfil tecnológico de TI, a partir del 2025, independientemente del tipo de gestión, comité o unidad de TI sea esta individual o corporativa que la entidad defina.

b) Las fechas de remisión del primer perfil de las sociedades corredoras de seguros serán comunicadas por la SUGESE mediante acto administrativo en el tercer trimestre del 2024, a través de los canales oficiales.

3. Auditoría Externa de TI:

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

Disposición transitoria sexta. Perfil tecnológico

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

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

Disposición transitoria séptima. Implementación de las modificaciones reglamentarias

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

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

Sin perjuicio de lo anterior, para la elaboración de los planes de implementación se deben considerar los plazos establecidos en los siguientes artículos de la modificación reglamentaria y en sus lineamientos generales, a fin de que la ejecución de los planes permita el cumplimiento de los plazos establecidos en dichos artículos:

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

Artículo 40. Comunicado de incidentes a los clientes

Artículo 41. Información histórica de incidentes de seguridad de la información y seguridad cibernética

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

A partir del sexto mes de la entrada en vigor del reglamento, los planes de implementación para atender brechas deberán estar a disposición de las Superintendencias cuando estas lo requieran. Dichos planes podrán ser considerados para definir los alcances de la auditoría externa de TI o ser considerados como parte de la evaluación de las auditorías externas de TI."

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

"Resolución

05 DE agosto del 2024
SGF-2377-2024
SP-R-2236-2024
SGS-0844-2024
SGV-C03/0-1318
SGF-PUBLICO

Dirigida a:

Supervisados por SUGEF:

- *Bancos Comerciales del Estado*
- *Bancos Creados por Leyes Especiales*
- *Bancos Privados*
- *Empresas Financieras no Bancarias*
- *Otras Entidades Financieras*
- *Organizaciones Cooperativas de Ahorro y Crédito*
- *Asociaciones Mutualistas de Ahorro y Crédito*

Supervisados por SUGEVAL:

- *Puestos de bolsa y sociedades administradoras de fondos de inversión*
- *Bolsas de valores*
- *Sociedades de compensación y liquidación*
- *Proveedores de precio*
- *Entidades que brindan servicios de custodia*
- *Centrales de valores*
- *Sociedades titularizadoras y fiduciarias*
- *Entidades de registros centralizados de letras de cambio y pagarés electrónicos*

Supervisados por SUGESE:

- *Entidades aseguradoras y reaseguradoras*
- *Sucursales de entidades aseguradoras extranjeras*
- *Sociedades corredoras de seguros*

Supervisados por SUPEN:

- *Operadoras de pensiones complementarias*
- *Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social*
- *Fondos complementarios creados por leyes especiales o convenciones colectivas*

***Asunto**: Modificación integral a los Lineamientos Generales del Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24.*

La Superintendencia General de Entidades Financieras, la Superintendencia General de Valores, la Superintendencia de Pensiones y la Superintendencia General de Seguros.

Considerando,

1. *El Consejo Nacional de Supervisión del Sistema Financiero, mediante artículos 8 y 9 de las actas de sesiones 1876-2024 y 1877-2024, celebradas el 15 de julio del 2024, aprobó el Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24, publicado en el Alcance N. 130 del diario oficial La Gaceta N.134 del 22 de julio del 2024.*

i. *El artículo 5 del Reglamento General de Gobierno y Gestión de la Tecnología de Información habilita a los Superintendentes para emitir los Lineamientos Generales necesarios para su aplicación.*

ii. *Para este efecto, los Lineamientos Generales deben definir los aspectos necesarios para la aplicación del Reglamento General de Gobierno y Gestión de la Tecnología de Información según lo establecido en esa normativa.*

Disponen:

Aprobar la modificación integral de los Lineamientos Generales del Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24, de conformidad con el texto que se incluye a continuación:

"Lineamientos Generales al Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24

***Objetivo general**: Presentar los elementos necesarios que guían a las entidades y empresas supervisadas en la aplicación de las disposiciones establecidas en el Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24.*

Sección I. Lineamientos relacionados con el reconocimiento de la gestión de TI, del Comité de TI o sus funciones equivalentes como corporativos

***Objetivo:** Establecer las condiciones para tipificar la gestión de TI, el Comité de TI o sus funciones equivalentes como corporativos, así como el plazo de respuesta de las solicitudes de permiso para tipificar la gestión de TI como corporativa.*

1. ***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:***

   a) Alguna de las entidades o empresas supervisadas preste los servicios de TI a otras entidades o empresas de su mismo grupo o conglomerado financiero.

   b) Se implementan de forma centralizada las siguientes funciones:

      i. Aprobación de los objetivos e indicadores estratégicos de TI.

      ii. Aprobación de las políticas y procedimientos de TI.

      iii. Ejecución de las acciones para el logro de los objetivos y políticas, así como la aplicación de los procedimientos.

      iv. Gestión de los bienes y servicios de TI tercerizados.

      v. Suscripción de los contratos y acuerdos de nivel de servicio de TI de las entidades y empresas supervisadas.

      vi. Establecimiento de estructuras y funciones de gobierno, gestión y control de TI.

      vii. Asignación de los presupuestos, el control de la ejecución presupuestaria y la aplicación de las directrices presupuestarias.

2. ***El plazo de respuesta de las solicitudes de permiso para tipificar la gestión de TI como corporativa es el siguiente:***

   a) Las solicitudes de permiso remitidas por los grupos y conglomerados financieros al supervisor responsable para que su gestión de TI sea tipificada como corporativa, serán resueltas en el plazo de veinte días hábiles contados a partir de la recepción de la solicitud.

Sección II. Lineamientos relacionados con el modelo de clasificación de los activos de información

Objetivo: *Establecer las pautas para la implementación del modelo de clasificación de los activos de información.*

1. ***Clasificación de los activos de información. Las entidades y empresas supervisadas clasificarán los activos de información de la siguiente forma:***

   a) 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. *Se revelan en el perfil tecnológico a través de los formularios: activos de información y procesos de negocio.*

b) *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. *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.*

Sección III. Lineamientos relacionados con el modelo de clasificación de acceso y uso de los activos de información y datos utilizado para etiquetar dichos activos según su nivel de confidencialidad

Objetivo: *Establecer las pautas para la implementación del modelo de acceso y uso de los activos de información y datos para etiquetar dichos activos según su nivel de confidencialidad.*

1. Clasificación de acceso y uso de los activos de información y datos

a) Las entidades y empresas supervisadas, como parte de sus políticas sobre gestión de activos, clasificarán y etiquetarán, según el nivel de confidencialidad, los activos de información (cuando corresponda según la naturaleza y el riesgo del activo), de conformidad con los siguientes criterios:

Clasificación del acceso y uso de la información y los datos:				
	Uso público	***Uso interno***	***Uso confidencial[1]***	***Uso sensible***
Descripción:	*No hay restricciones legales o reglamentarias, tanto internas como externas, que limiten el acceso o uso de los activos de información y los datos. No se requiere medidas de protección especiales.[2]*	*El acceso o uso de los activos de información y los datos se concede a los custodios de los activos de información y los datos, con el propósito de llevar a cabo las funciones y actividades inherentes a la institución. No se comparte con externos sin razón o autorización válida.*	*Además de las características de "Uso interno", el acceso o uso están restringidos al puesto o rol asignado, así como a las tareas específicas dentro del proceso y equipo de trabajo correspondiente.[3]*	*Además de las características de "Uso confidencial", el acceso o uso están restringidos y serán explícitamente controlados y asignados considerando la sensibilidad de la información.[4]*

Sección IV. Lineamientos relacionados con las pautas para la implementación de los controles para la adquisición o el desarrollo del ciclo de vida del software y la codificación segura

Objetivo: *Establecer las pautas para la implementación de los controles relacionados con la adquisición o el desarrollo del ciclo de vida del software y la codificación segura, las cuales, serán consideradas para el caso de las aplicaciones vigentes o para nuevas adquisiciones o desarrollos.*

[1] Uso confidencial es homologado a las clasificaciones propietario o restringido.
[2] Incluye datos personales de uso público o acceso irrestricto así declarados expresamente por leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.
[3] Incluye datos personales de acceso restringido que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.
[4] Incluye los datos sensibles, relativos al fuero íntimo de la persona, por ejemplo, los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

1. Las siguientes pautas serán implementadas en función de los riesgos identificados:

a) Solicitar que los proveedores de aplicaciones, de los sistemas de información y de las soluciones tecnológicas, incluyan controles de seguridad de la información y de seguridad cibernética en sus productos, cuando así corresponda en función de los riesgos identificados por la entidad o empresa supervisada o de los riesgos de los citados proveedores.

b) En los casos en que la entidad o empresa supervisada diseñe, desarrolle, implemente o provea aplicaciones, sistemas de información o soluciones tecnológicas, valorará lo siguiente:

i. Dentro del ciclo de vida del desarrollo del software, se consideren controles de seguridad de la información y seguridad cibernética para las interfases de programación (API), servicios web, aplicaciones (apps) y bases de datos que procesan y almacenan información de la entidad o empresa supervisada, desde la fase de diseño, como un requerimiento o funcionalidad adicional.

ii. Definición de ambientes aislados y controlados para cada una de las fases del desarrollo del ciclo de software.

iii. Uso de herramientas o métodos de ofuscamiento que se encargan de modificar los datos para que sean válidos en ambientes distintos al de producción.

vi. Los controles necesarios para la codificación segura de cualquier otra tecnología emergente que se implemente.

c) Validar que las aplicaciones, los sistemas de información, las soluciones adquiridas o desarrolladas a lo interno de la entidad o empresa supervisada, en función de sus riesgos, cumplan con los principios y los aspectos de seguridad de la información que se detallan, a continuación:

i. Confidencialidad.

ii. Integridad.

iii. Disponibilidad.

iv. No repudio.

v. Defensa en profundidad.

vi. Confianza cero.

vii. Mínima exposición al riesgo.

viii. Necesidad del mínimo conocimiento.

ix. Accesos con privilegio mínimo.

x. Segregación y separación de funciones.

xi. *Seguridad por diseño.*

xii. *Encriptación de datos en reposo y en tránsito.*

xiii. *Autenticación con múltiples factores.*

xiv. *Seguridad por defecto.*

d) *Identificar y gestionar los flujos de datos que trasladen información de la entidad o empresa supervisada a proveedores de bienes y servicios de TI o del negocio y viceversa. Lo anterior, a fin de establecer los controles que aseguren su confidencialidad, integridad y disponibilidad en el origen, en el tránsito y en el destino.*

e) *Mantener la mayor cantidad de datos fuera del alcance de terceros sin dañar la funcionalidad de las aplicaciones, de los sistemas de información o de las soluciones de negocio.*

f) *Usar protocolos de comunicación segura que resguarden la privacidad de la información.*

g) *Realizar una evaluación de los riesgos asociados para implementar los controles de seguridad de la información y de seguridad cibernética cuando se utilice software libre.*

h) *Cuando se tengan sistemas legados y no se puedan implementar las medidas indicadas anteriormente, las entidades y empresas supervisadas podrán implementar los controles compensatorios que permitan mitigar los riesgos en caso de no implementar dichos controles. En todo caso, las entidades y empresas supervisadas valorarán la migración de sistemas legados a plataformas seguras de conformidad con lo establecido en la estrategia de la organización, así como su apetito, capacidad y tolerancia de riesgo.*

Sección V. Lineamientos relacionados con el diseño de los contratos y acuerdos de nivel de servicio

Objetivo: *Establecer los elementos que las entidades y empresas supervisadas 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. (Estos lineamientos no aplican para bienes o servicios suministrados por proveedores de computación en la nube ni para contratos de adhesión).*

1. Cláusulas

a) *Los contratos y acuerdos de nivel de servicio de TI que celebren las entidades y empresas supervisadas con sus proveedores contendrán las siguientes cláusulas:*

"Artículo XX. Obligaciones de la unidad de TI/proveedor de TI frente a los supervisores de las entidades y empresas.

(nombre de la unidad de TI/proveedor de TI) se obliga a suministrar a (nombre de la Superintendencia) y al auditor externo de TI toda información que le sea requerida por estos, así como todas las facilidades requeridas en la supervisión de TI, de acuerdo con la reglamentación emitida por el Consejo Nacional de Supervisión del Sistema Financiero de la República de Costa Rica y sus Lineamientos Generales. Asimismo, (nombre de la unidad de TI/proveedor de TI) se obliga a continuar brindando los servicios de TI contratados, aun en el caso de intervención de alguna entidad o empresa supervisada por parte de un órgano supervisor costarricense.

Artículo XXX. Obligaciones de los proveedores frente a los requerimientos de auditorías externas de TI.

(nombre de la unidad de TI/proveedor de TI) se compromete a ejecutar una auditoría externa de TI, cuando así sea requerida por la entidad o empresa supervisada. El alcance, plazo del estudio, plazo de ejecución y entrega podrán ser definidos por la entidad o empresa supervisada de conformidad con las solicitudes de las Superintendencias".

2. Elementos

Los elementos que las entidades y empresas supervisadas incorporarán en el diseño de los contratos y acuerdos de nivel de servicio de TI, según lo requieran de conformidad con la naturaleza del bien o servicio tercerizado, así como el tipo de proveedor, son los siguientes:

a) Aspectos para considerar:

1 Generalidades del servicio:

1.1 Código del servicio.

1.2 Nombre del servicio.

1.3 Descripción del servicio.

1.4 Persona responsable del servicio, fecha, hora y lugar de autorización del SLA/OLA/UC.

2 Información de autorización:

2.1 Nombre, puesto y contacto del gestor del servicio.

2.2 Información del cliente que recibe el servicio (nombre, lugar, entre otros).

3 Duración del acuerdo:

3.1 Fecha de inicio y fin del acuerdo.

3.2 Reglas sobre la terminación del acuerdo.

4 Requerimientos del negocio que satisface:

4.1 Descripción de los procesos de negocio que apoya el servicio.

4.2 Descripción de los servicios de negocio que apoya el servicio.

4.3 Descripción de resultados o de sus proyecciones en términos de utilidad.

4.4 Descripción de resultados o de sus proyecciones en términos de garantía.

5 Criticidad del servicio y equipos que lo soportan:

5.1 Identificación de los equipos esenciales para el negocio conectados con el servicio.

5.2 Estimación del impacto en el negocio causado por una pérdida de servicio o activos.

6 Contratos y otros:

6.1 Referencia a otros contratos, SLA, OLA, UC adicionales.

7 Tiempo del servicio:

7.1 Horario que estará disponible el servicio.

7.2 Excepciones.

7.3 Periodo de mantenimiento.

8 Tipos y niveles de apoyo requeridos:

8.1 Apoyo in situ:

8.1.1 Área/ localizaciones a las que se debe tener acceso.

8.1.2 Tipos de usuarios.

8.1.3 Aplicaciones o componentes de infraestructura que apoya el servicio.

8.1.4 Tiempos de reacción y resolución de incidentes o problemas.

8.2 Apoyo extra situ:

8.2.1 Área/ localizaciones a las que se debe tener acceso.

8.2.2 Tipos de usuarios.

8.2.3 Aplicaciones o componentes de infraestructura que apoya el servicio.

8.2.4 Tiempos de reacción y resolución de incidentes o problemas.

9 Requisitos/ metas de nivel de servicio:

9.1 Metas de disponibilidad:

9.1.1 Condiciones bajo las cuales se considera que el servicio no está disponible.

9.1.2 Metas de disponibilidad.

9.1.3 Metas de confiabilidad.

9.1.4 Metas de sustentabilidad.

9.1.5 Metas de integridad.

9.1.6 Metas de confidencialidad.

9.1.7 Tiempos de inactividad para mantenimiento.

9.1.8 Restricciones en el mantenimiento.

9.1.9 Procedimientos para anunciar interrupciones al servicio (planificados/ sin planificar).

9.1.10 Requisitos referentes a los informes de disponibilidad.

9.2 Metas de capacidad/ desempeño:

9.2.1 Capacidad requerida (límite más bajo/ alto) para el servicio:

9.2.1.1 Números y tipos de transacciones.

9.2.1.2 Números y tipos de usuarios.

9.2.1.3 Ciclos del negocio.

9.2.2 Tiempo de respuesta de aplicaciones.

9.2.3 Requisitos de escalabilidad.

9.2.4 Requisitos referentes a los informes de capacidad y desempeño.

9.3 Compromisos de continuidad del servicio (disponibilidad del servicio en caso de una contingencia o desastre):

9.3.1 Tiempo en que un nivel de servicio definido debe ser restablecido.

9.3.2 Tiempo en que los niveles normales de servicio deben ser restaurados.

10 Estándares:

10.1 Listado detallado de los estándares técnicos y la especificación de la interfaz del servicio técnico.

11 Responsabilidades:

11.1 Deberes del proveedor de bienes o servicios.

11.2 Deberes del cliente.

11.3 Responsabilidades de los usuarios del servicio.

11.4 Aspectos de la seguridad de TI que se deben observar al usar el servicio.

12 Costos y precios:

12.1 Costos detallados de proveer el servicio.

13 Reglas para penalidades/ reversiones.

14 Historial de cambios.

15 Anexos.

Sección VI. Lineamientos relacionados con los atributos de los controles de la seguridad de la información y la seguridad cibernética revelados en la declaración de aplicabilidad para el diseño e implementación del sistema de gestión de seguridad de la información

***Objetivo**: Establecer los atributos que especificarán los controles de la seguridad de la información y la seguridad cibernética revelados en la declaración de aplicabilidad para el diseño e implementación del sistema de gestión de seguridad de la información.*

1. Los controles que se revelen en la declaración de aplicabilidad para el diseño e implementación del sistema de gestión de seguridad de la información especificarán los siguientes atributos:

a) Identificador del control:

Identificador único del control.

b) Descripción del control:

Descripción general del control.

c) Objetivo del control:

Objetivo del control.

d) Justificación de la selección del control:

Justificación de la aplicabilidad o no aplicabilidad del control y su referencia a la declaración del apetito de riesgo en la entidad o empresa supervisada. Lo anterior, cuando corresponda.

e) Estado de implementación del control:

Revela el estado de implementación: planificación, diseño, operación.

f) Tipo de control:

Permite ver los controles desde la perspectiva de cuándo y cómo el control modifica el riesgo con respecto a la ocurrencia de un incidente de seguridad de la información o de seguridad cibernética identificado y se clasifica en:

i. Preventivo.

ii. Detectivo.

iii. Correctivo.

g) Propiedades de la seguridad de la información:

Permite ver los controles desde la perspectiva de qué características de la información el control contribuirá a preservar, a saber:

i. Confidencialidad.

ii. Integridad.

iii. Disponibilidad.

h) Funciones de seguridad cibernética relacionadas:

Permite ver los controles desde la perspectiva de la asociación de los controles a las funciones de seguridad cibernética:

i. Gobernar.

ii. Identificar.

iii. Detectar.

iv. Proteger.

v. Recuperar.

vi. Responder.

i) Capacidades operacionales de la entidad o empresa supervisada:

Permite ver los controles desde la perspectiva de las capacidades de seguridad de la información de la entidad o empresa supervisada:

i. Gobernanza.

ii. Gestión de activos.

iii. Protección de la información.

iv. Seguridad de los recursos humanos.

v. Seguridad física.

vi. Seguridad de sistemas y redes.

vii. Seguridad de las aplicaciones.

viii. Configuración segura.

ix. Gestión de la identidad y del acceso.

x. Gestión de amenazas y vulnerabilidades.

xi. Continuidad.

xii. Seguridad de las relaciones con los proveedores.

xiii. Cumplimiento legal.

xiv. Gestión de eventos de seguridad de la información.

xv. Aseguramiento de la información.

j) Dominios de seguridad:

Permite ver los controles desde la perspectiva de cuatro dominios de seguridad de la información, a saber:

i. Gobernanza y ecosistema.

ii. Protección.

iii. Defensa.

iv. Resiliencia.

2. Cuando el supervisor requiera conocer los controles relacionados con las funciones para la evaluación de la gestión de riesgos de seguridad cibernética (detalladas en el Anexo 4 de los presentes lineamientos), el informe de la auditoría externa de TI contendrá un apartado que muestre dichos controles. Lo anterior, se realizará desde la perspectiva de la asociación de los controles a las funciones de seguridad cibernética indicada en el inciso h) del numeral anterior.

Sección VII. Lineamientos relacionados con las fases de la gestión de incidentes de seguridad de la información y seguridad cibernética

***Objetivo**: Diseñar e implementar las fases de la gestión de incidentes de seguridad de la información y seguridad cibernética.*

1. Las fases de la gestión de incidentes de seguridad de la información y seguridad cibernética que se incorporarán en el proceso para la gestión de incidentes son las siguientes:

Fase I. Preparación

1. Esta fase incorpora aspectos relacionados con preparar, mejorar o sustentar la gestión de incidentes de seguridad de la información y seguridad cibernética.

2. Contempla la creación y formación de una capacidad de gestión y respuesta a incidentes de seguridad de la información y seguridad cibernética, alineada a la gestión de incidentes de la entidad o empresa supervisada, que incluye al menos:

a) Coordinar la planificación y el diseño

Permite realizar las actividades de coordinación, planificación y diseño considerando, al menos, lo siguiente:

i. Identificar requerimientos de gestión de incidentes.

ii. Establecer la visión y la misión de la gestión.

iii. Obtener financiamiento y patrocinio.

iv. Desarrollar un plan de implementación.

b) Coordinar la implementación

Permite realizar las actividades de coordinación para la implementación de los aspectos planificados y de la gestión de incidentes considerando, al menos, lo siguiente:

i. Desarrollar políticas, procesos y planes.

ii. Definir la clasificación y categorización de incidentes de conformidad con las disposiciones de los presentes lineamientos.

iii. Alinear la gestión de incidentes al plan de continuidad del negocio, recuperación de desastres y atención ante una crisis.

iv. Evaluar la capacitación, prueba y evaluación de la gestión de incidentes.

v. Implementar y gestionar los recursos incluyendo el talento humano, las herramientas y tecnología para la gestión de incidentes.

vi. Definir los mecanismos para comunicarse con las partes internas y externas antes, durante y después de la ocurrencia de un incidente.

vii. Definir las políticas y procedimientos que permitan recopilar pruebas o evidencias ante un proceso disciplinario, judicial o un análisis forense.

viii. *Ejecutar, cuando así lo amerite el caso, las actividades de respuesta, contención, mitigación, recopilación de pruebas y recuperación en coordinación con los procesos o áreas legales. Lo anterior, considerando que podrían requerir asesoría por temas de investigación, crímenes cibernéticos, responsabilidad civil, propiedad intelectual, privacidad de datos, leyes, regulación, entre otros.*

3. *Considera la evaluación del estado actual de la capacidad de respuesta a incidentes, incluyendo actividades tales como: encuestas al Órgano de Dirección, a la Alta Gerencia, a los encargados de las áreas de TI; autoevaluaciones o evaluaciones y auditorías externas, así como las lecciones aprendidas como resultado de incidentes anteriores y documentados mediante la Fase IV. Actividades post incidente.*

Fase II. Detección y análisis:

1. *Esta fase incorpora aspectos relacionados con proteger, detectar o realizar el triage (proceso de clasificación, categorización, correlación, así como la priorización y asignación de reportes, eventos, incidentes, entre otros) de los incidentes de seguridad de la información y seguridad cibernética.*

2. *Permite iniciar con la detección de la amenaza una vez que ha penetrado en la entidad o empresa supervisada, considerando lo siguiente:*

   a) *Ser ejecutada por la propia entidad o empresa supervisada o por terceros que generarán el correspondiente aviso.*

   b) *Permite proteger la reputación, marca, infraestructuras o datos de la organización y de tecnologías de información.*

   c) *Propone mejoras sobre los planes.*

   d) *Permite detectar eventos, incidentes y anomalías de forma proactiva, reactiva y el comunicado oportuno de reportes.*

   e) *Permite establecer el triage.*

   f) *En esta fase se realiza el comunicado de incidentes a la respectiva Superintendencia.*

Fase III. Contención, mitigación y recuperación:

1. *Esta fase incorpora aspectos relacionados con la respuesta, contención, mitigación y recuperación de incidentes de seguridad de la información y seguridad cibernética.*

2. *Los incidentes de seguridad de la información y seguridad cibernética son atendidos según su criticidad considerando entre otros aspectos:*

   a) *Respuesta al incidente a nivel técnico:*

i. *En primera instancia, se mitigará el impacto del incidente, luego, se eliminará de los sistemas afectados, se tratará de recuperar el sistema al modo de funcionamiento normal. En caso de persistir, se realiza el análisis de la amenaza, de cuyos resultados se desprenderán nuevos mecanismos de contención y erradicación; lo anterior, cuando corresponda según el tipo de incidente.*

ii. *Se pueden utilizar los playbooks[5] establecidos por organismos gubernamentales o por los principales fabricantes y proveedores de bienes y servicios de TI.*

b) *Respuesta al incidente a nivel gerencial:*

i. *Ejecutar las actividades de intervención, notificación, interacción, escalamiento y coordinación de esfuerzos (internos y externos) para la respuesta, contención, mitigación y recuperación de incidentes; lo anterior, cuando corresponda según el tipo de incidente e impacto.*

ii. *Comunicar a los clientes aquellos incidentes que afecten la confidencialidad o integridad de su información.*

iii. *En esta fase se remiten los informes de incidentes a la respectiva Superintendencia cuando esta lo solicite.*

c) *Respuesta al incidente a nivel legal:*

Ejecutar las actividades de respuesta, contención, mitigación y recuperación relacionadas con temas de investigación, proceso legal, responsabilidad civil, propiedad intelectual, privacidad de datos, leyes y regulación, entre otros.

d) *Se ejecutan los planes de continuidad del negocio, recuperación de desastres y atención ante una crisis en los casos que lo requieran.*

Fase IV. Actividades post incidente:

1. *Esta fase incorpora aspectos relacionados con las actividades post incidente en las entidades y empresas supervisadas. Los insumos obtenidos como resultado de la ejecución de esta fase pueden ser utilizados posteriormente para mejorar la respuesta a incidentes en la Fase I Preparación. Dichos aspectos son los siguientes:*

a) *Gestionar las lecciones aprendidas que permitan mejorar los controles de la entidad o empresa supervisada.*

b) *Recolectar los datos para la información histórica de incidentes.*

[5] Guías esenciales que orientan a los equipos de seguridad para actuar con confianza y eficacia frente a las amenazas cibernéticas, asegurando así la protección continua de los activos digitales de la organización.

c) *Custodia de la evidencia en los casos que se requiera.*

d) *Emitir el informe post incidente y el comunicado a los clientes cuando corresponda.*

Sección VIII. Lineamientos relacionados con la clasificación del impacto de una brecha de seguridad de información o de seguridad cibernética

1. Cuando se identifique una brecha de seguridad de información o de seguridad cibernética, el impacto potencial de dicha brecha se establecerá de conformidad con la siguiente clasificación:

Impacto potencial	*Descripción*
Nulo	*No hay impacto, los activos de información son de uso o acceso público.*
Bajo	*Se presenta una pérdida de confidencialidad, integridad o disponibilidad que tenga un efecto adverso limitado en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*
Moderado	*Se presenta la pérdida de confidencialidad, integridad o disponibilidad que tenga un efecto adverso grave en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*
Alto	*Se presenta una pérdida de confidencialidad, integridad o disponibilidad que tenga un efecto adverso grave o catastrófico en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*

Sección IX. Lineamientos relacionados con la clasificación para el registro de los incidentes de seguridad de la información y seguridad cibernética

Objetivo: *Establecer la clasificación para el registro de incidentes de seguridad de la información y seguridad cibernética y sus tipos de incidentes.*

1. Clasificación para el registro de los incidentes de seguridad de la información y seguridad cibernética

Clasificación	*Tipo de incidente*	*Descripción práctica*
Contenido abusivo	*Correo masivo no solicitado (SPAM)*	*Correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.*
	Delito de odio	*Contenido difamatorio o discriminatorio. Ejemplo: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.*
	Pornografía infantil, contenido sexual o violento inadecuado	*Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.*
Contenido dañino	*Sistema infectado*	*Sistema infectado con programa maligno. Ejemplo: Sistema, computadora o teléfono móvil infectado con un rootkit.*
	Servidor C&C (Mando y Control)	*Conexión con servidor de Mando y Control (C&C) mediante programa maligno o sistemas infectados.*
	Distribución de programa maligno	*Recurso usado para distribución de programa maligno. Ejemplo: recurso de una entidad o empresa supervisada empleado para distribuir programa maligno.*
	Configuración de programa maligno	*Recurso que aloje ficheros de configuración de programa maligno. Ejemplo: ataque de webinjects para troyano.*

Clasificación	Tipo de incidente	Descripción práctica
Obtención de información	*Escaneo de redes (scanning)*	*Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplo: peticiones DNS, ICMP, SMTP, escaneo de puertos.*
	Análisis de paquetes (sniffing)	*Observación y grabación del tráfico de redes.*
	Ingeniería social	*Recopilación de información personal sin el uso de la tecnología. Ejemplo: mentiras, trucos, sobornos, amenazas.*
Intento de intrusión	*Explotación de vulnerabilidades conocidas*	*Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades. Ejemplo: desbordamiento de buffer, puertas traseras, Cross site scripting (XSS).*
	Intento de acceso con vulneración de credenciales	*Múltiples intentos de vulnerar credenciales. Ejemplo: intentos de ruptura de contraseñas, ataque por fuerza bruta.*
	Ataque desconocido	*Ataque empleando exploit desconocido.*
Intrusión	*Cuenta comprometida*	*Compromiso exitoso de un sistema por el uso de una cuenta privilegiada o no privilegiada comprometida.*
	Compromiso de aplicaciones	*Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.*
	Robo	*Intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos.*
Disponibilidad	*Denegación de servicio (DoS)*	*Ataque de denegación de servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.*
	Denegación distribuida de servicio (DDoS)	*Ataque de denegación distribuida de servicio. Ejemplo: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.*
	Mala configuración	*Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ejemplo: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.*
	Sabotaje	*Sabotaje físico. Ejemplo: cortes de cableados de equipos o incendios provocados.*
	Interrupciones	*Interrupciones por causas ajenas. Ejemplo: desastre natural.*
Compromiso de la información	*Acceso no autorizado a información*	*Acceso no autorizado a información. Ejemplo: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.*
	Modificación no autorizada de información	*Modificación no autorizada de información. Ejemplo: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.*
	Pérdida de datos	*Pérdida de información Ejemplo: pérdida por fallo de disco duro o robo físico.*
	Uso no autorizado de recursos	*Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.*
Fraudes	*Derechos de autor*	*Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplo: Warez.*
	Suplantación	*Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.*
Vulnerabilidades	*Phishing*	*Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.*
	Criptografía débil	*Servicios accesibles públicamente que no presentan o puedan presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.*
	Amplificador DDoS	*Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplo: DNS open-resolvers o Servidores NTP con monitorización monlist.*
	Servicios con acceso potencial no deseado	*Ejemplo: Telnet, RDP o VNC.*
	Revelación de información	*Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ejemplo: SNMP o Redis.*
	Sistema vulnerable	*Sistema vulnerable. Ejemplo: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.*
Otros	*Otros*	*Todo aquel incidente que no tenga cabida en ninguna categoría anterior.*
	Amenazas Persistentes Avanzadas (APT por sus siglas en inglés)	*Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.*

Sección X. Lineamientos relacionados con la clasificación del impacto de los incidentes de seguridad de la información y seguridad cibernética

***Objetivo**: Establecer las pautas relacionadas con la clasificación del impacto de los incidentes de seguridad de la información y seguridad cibernética.*

1. Clasificación del impacto

a) Cuando sea necesario, las entidades y empresas supervisadas evaluarán el impacto en caso de presentarse incidentes de seguridad de la información y seguridad cibernética, de conformidad con los siguientes niveles de impacto:

Propiedad de seguridad de la información	***Nivel de impacto / Descripción***		
	Bajo	***Moderado***	***Alto***
Confidencialidad	*La divulgación o acceso no autorizado de información puede tener un efecto limitado en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*	*La divulgación o acceso no autorizado de información puede tener un efecto grave en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*	*La divulgación o acceso no autorizado de información puede tener un efecto severo o catastrófico en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*
Integridad	*La modificación o destrucción no autorizada de la información puede tener un efecto limitado en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*	*La modificación o destrucción no autorizada de información puede tener un efecto grave en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*	*La modificación o destrucción no autorizada de información puede tener un efecto severo o catastrófico en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*
Disponibilidad	*La interrupción del acceso o uso de la información o de un sistema de información puede tener un efecto limitado en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*	*La interrupción del acceso o uso de la información o de un sistema de información puede tener un efecto grave en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*	*La interrupción del acceso o uso de la información o de un sistema de información puede tener un efecto severo o catastrófico en las operaciones, los activos de información o el personal de la entidad o empresa supervisada.*

Sección XI. Lineamientos relacionados con la comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias

***Objetivo**: Establecer la descripción, plazo y contenido del comunicado de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias, así como los tipos, plazos y formatos de los informes de comunicación de incidentes de seguridad de la información y seguridad cibernética.*

1. Comunicado inicial

a) Comunicado inicial:

i. ***Descripción****: Comunicado oficial de la entidad o empresa supervisada que se remite a la respectiva Superintendencia, el cual, revela la ocurrencia de un incidente de seguridad de la información o de seguridad cibernética cuyo impacto es "moderado" o "alto".*

ii. ***Plazo****: El Comunicado inicial será remitido a la respectiva Superintendencia sin demora y a más tardar ocho horas naturales contadas a partir de identificado el incidente y de establecido su impacto o afectación como "moderado" o "alto".*

iii. ***Contenido****: Las entidades y empresas supervisadas definirán el contenido mínimo del comunicado, considerando que este sea oportuno, claro y con un alcance apropiado en función del incidente.*

2. Tipos y plazos de remisión de informes de incidentes

a) Tipo: ***Informe de atención de incidentes***

i. ***Descripción****: Informe oficial de la entidad o empresa supervisada donde se detalla el incidente de seguridad de la información o de seguridad cibernética revelado en el Comunicado inicial, así como la atención de dicho incidente.*

ii. ***Plazo****: La solicitud del Informe de atención de incidentes y el plazo para la remisión de dicho informe serán comunicados mediante los canales oficiales de cada Superintendencia.*

b) Tipo: ***Informe de seguimiento de atención de incidentes***

i. ***Descripción****: Informe de seguimiento de las actividades que fueron detalladas mediante el "Informe de atención de incidentes" para atender el incidente de seguridad de la información o seguridad cibernética.*

ii. ***Plazo:*** *La solicitud del Informe de seguimiento de atención de incidentes y el plazo de remisión de dicho informe serán comunicados mediante los canales oficiales de cada Superintendencia.*

c) Tipo: ***Informe post actividades de incidentes***

i. ***Descripción****: Incluye, al menos, reporte de costes, los reportes técnicos y de análisis forense, así como lecciones aprendidas.*

ii. ***Plazo:*** *La solicitud del Informe post actividades de incidentes y el plazo para la remisión de dicho informe serán comunicados mediante los canales oficiales de cada Superintendencia.*

3. Formatos de los informes de incidentes

Los siguientes formatos son una guía de referencia para la entidad o empresa supervisada a fin de homologar el contenido mínimo de los informes de incidentes. Queda a discreción de la entidad o empresa supervisada incorporar información o secciones adicionales.

Cuando algún aspecto de los indicados en los formatos de los informes no se pueda definir en el momento de la elaboración del informe, la entidad o empresa supervisada indicará dicha salvedad.

a) Formato del Informe de atención de incidentes:

1. El Informe de atención de incidentes contendrá, al menos, los siguientes aspectos:

i. Portada:

1. Nombre de la entidad o empresa supervisada.

2. Título del informe.

3. Nombre y puesto de la persona que elaboró el informe.

4. Número consecutivo de registro del incidente (lo define la entidad).

5. Fecha del informe.

ii. Contenido del Informe de atención de incidentes:

1. Plan de trabajo inicial:

a. Plan de trabajo, hoja de ruta, o cronograma general que incluya al menos, las actividades, estado de dichas actividades (planificado, en proceso o finalizado), porcentaje de avance, responsables y plazos.

2. Descripción del responsable de atender el incidente:

a. Nombre y puesto de la persona responsable de atender el incidente.

b. Correo electrónico y número telefónico.

c. Localización física de la persona.

3. Descripción de equipos de trabajo:

Nombres y puestos de las personas (internas/externas) y rol de cada miembro dentro del equipo que conforman la función de respuesta para la atención del incidente, continuidad de las operaciones y tratamiento de la crisis.

4. *Descripción de lo identificado en las etapas de Detección y Análisis:*

   a. *Descripción general del incidente.*

   b. *Vectores de ataque.*

   c. *Clasificación del incidente según la sección IX de los presentes lineamientos.*

   d. *Descripción del impacto según las categorías.*

   e. *Cualquier otro aspecto que la entidad o empresa supervisada considere necesario revelar.*

b) *Formato del Informe de seguimiento de atención de incidentes*

1. *El Informe de seguimiento de atención de incidentes contendrá, al menos, los siguientes aspectos:*

   i. *Portada:*

      1. *Nombre de la entidad o empresa supervisada.*

      2. *Título del informe.*

      3. *Nombre y puesto de la persona que elaboró el informe.*

      4. *Número consecutivo de registro del incidente (lo define la entidad).*

      5. *Fecha del informe.*

   ii. *Contenido del Informe de seguimiento de atención de incidentes:*

      1. *Plan de trabajo inicial:*

         a. *Plan de trabajo, hoja de ruta, o cronograma general que incluya, al menos, las actividades, estado de dichas actividades (planificado, en proceso o finalizado), porcentaje de avance, responsables y plazos.*

      2. *Descripción del responsable de atender el incidente:*

         a. *Nombre y puesto de la persona responsable de atender el incidente.*

         b. *Correo electrónico y número telefónico.*

         c. *Localización física de la persona.*

      3. *Descripción de equipos de trabajo:*

         a. *Nombres y puestos de las personas (internas/externas) y rol de cada miembro dentro del equipo que conforman la*

función de respuesta para la atención del incidente, continuidad de las operaciones y tratamiento de la crisis.

4. *Descripción de lo identificado en las etapas de Detección y Análisis:*

   a. *Descripción general del incidente.*

   b. *Fecha y hora del evento.*

   c. *Vectores de ataque.*

   d. *Clasificación del incidente según la sección IX de los presentes lineamientos.*

   e. *Descripción del impacto según las categorías.*

   f. *Cualquier otro aspecto que la entidad o empresa supervisada considere necesario revelar.*

5. *Actualización del estado reportado en el Informe de atención de incidentes o en informes de seguimiento de incidentes previos, para comprender la situación actual o el avance de las medidas de la contención, mitigación y recuperación del incidente:*

   a. *Plan de trabajo (actualizado):*

      i. *Plan de trabajo, hoja de ruta, o cronograma general que incluya al menos, las actividades, estado de dichas actividades (planificado, en proceso o finalizado), porcentaje de avance, responsables y plazos.*

   b. *Resumen de las acciones para:*

      i. *Contención del incidente.*

   c. *Descripción de las actividades ejecutadas para:*

      i. *Mitigación del incidente.*

   d. *Descripción de las actividades ejecutadas para:*

      i. *Recuperación de los sistemas afectados.*

   e. *Descripción de otros aspectos que se considere necesario revelar.*

c) *Formato del Informe post actividades del incidente*

1. *El Informe post actividades del incidente contendrá, al menos, los siguientes aspectos:*

   i. *Portada:*

1. *Nombre de la entidad o empresa supervisada.*
2. *Título del informe.*
3. *Nombre y puesto de la persona que elaboró el informe.*
4. *Número consecutivo de registro del incidente (lo define la entidad).*
5. *Fecha del informe.*

ii. *Contenido del Informe de post actividades del incidente:*

1. *Plan de trabajo.*
    a. *Plan de trabajo, hoja de ruta, o cronograma general que incluya al menos, las actividades, estado de dichas actividades (planificado, en proceso o finalizado), porcentaje de avance, responsables y plazos.*
2. *Descripción del responsable de atender el incidente:*
    a. *Nombre y puesto de la persona responsable de atender el incidente.*
    b. *Correo electrónico y número telefónico.*
    c. *Localización física de la persona.*
3. *Descripción de equipos de trabajo:*
    a. *Nombres y puestos de las personas (internas/externas) y rol de cada miembro dentro del equipo que conforman la función de respuesta para la atención del incidente, continuidad de las operaciones y tratamiento de la crisis.*
4. *Descripción de lo identificado en las etapas de Detección y Análisis*
    a. *Descripción general del incidente.*
    b. *Fecha y hora del evento.*
    c. *Vectores de ataque.*
    d. *Clasificación del incidente según la sección IX de los presentes lineamientos.*
    e. *Descripción del impacto según las categorías.*
    f. *Cualquier otro aspecto que la entidad o empresa supervisada considere necesario revelar.*
5. *Actualización del estado reportado en el Informe de atención de incidentes o en informes de seguimiento de incidentes previos,*

para comprender la situación actual o el avance de las medidas de la contención, mitigación y recuperación del incidente:

a. Plan de trabajo (actualizado):

i. Plan de trabajo, hoja de ruta, o cronograma general que incluya, al menos, las actividades, estado de dichas actividades (planificado, en proceso o finalizado), porcentaje de avance, responsables y plazos.

b. Resumen de las acciones para:

i. Contención del incidente.

c. Descripción de las actividades ejecutadas para:

i. Mitigación del incidente.

d. Descripción de las actividades ejecutadas para:

i. Recuperación de los sistemas afectados.

e. Descripción de otros aspectos que se considere necesario revelar.

6. Informes técnicos:

a. Informes de análisis forenses.

b. Cualquier otro informe técnico.

7. Resumen del incidente:

a. ¿Cuándo comenzó el incidente?

b. ¿Cuándo se descubrió o detectó el incidente?

c. ¿Cuándo se realizó el comunicado inicial del incidente a la Superintendencia?

d. ¿Cuándo se resolvió el incidente?

e. ¿Cuándo se finalizó el incidente?

f. Ubicación física del incidente.

g. Origen/causa del incidente (si se conoce), incluidos nombres de host y direcciones IP.

h. Descripción del incidente (cómo se detectó, qué ocurrió).

i. Descripción de los recursos afectados (redes, hosts, aplicaciones, datos), incluidos los nombres de host de los sistemas y las direcciones IP.

j. Los vectores de ataque asociados al incidente e indicadores relacionados con el incidente (patrones de tráfico, claves de registro, etc.). Lo anterior, en caso de tener el dato.

k. Factores atenuantes.

l. Otras organizaciones contactadas (ejemplo: proveedor de software).

m. Comentarios generales.

8. Lecciones aprendidas:

a. ¿Cuál información se necesitaba antes para prevenir el incidente?

b. ¿Se tomaron medidas o acciones que podrían haber inhibido la recuperación?

c. ¿Qué harían diferente el personal y la Alta Gerencia la próxima vez que ocurra un incidente similar?

d. ¿Cómo se podría haber mejorado el intercambio de información con otras organizaciones?

e. ¿Cuáles acciones correctivas pueden prevenir incidentes similares en el futuro?

f. ¿Cuáles precursores o indicadores se deben vigilar en el futuro para detectar incidentes similares?

g. ¿Cuáles herramientas o recursos adicionales se necesitan para detectar, analizar y mitigar futuros incidentes?

Sección XII. Lineamientos relacionados con el contenido y plazo de conservación de la información histórica de los incidentes de seguridad de la información y seguridad cibernética

Objetivo: *Definir el contenido y plazo de conservación de la información histórica de incidentes de seguridad de la información y seguridad cibernética.*

1. Contenido y plazo de conservación de la información histórica de incidentes de seguridad de la información y seguridad cibernética

a) La información histórica de incidentes de seguridad de la información y seguridad cibernética contendrá los siguientes aspectos:

i. Número consecutivo de registro del incidente (lo define la entidad).

ii. *Fecha y hora de inicio del incidente.*

iii. *Fecha y hora de finalización del incidente.*

iv. *Duración de la interrupción.*

v. *Descripción del incidente.*

vi. *Causa Raíz.*

vii. *Solución.*

viii. *Impacto en el negocio.*

ix. *Costo estimado del incidente.*

x. *Cualquier otro aspecto que la entidad o empresa supervisada considere necesario revelar.*

b) *Plazo de conservación de la información histórica:*

i. *El plazo para la conservación de la información histórica de incidentes de seguridad de la información y seguridad cibernética es de al menos cinco años.*

Sección XIII. Lineamientos relacionados con las auditorías externas de TI

Objetivo: *Presentar los elementos necesarios que guiarán a las entidades y empresas supervisadas en la aplicación de las disposiciones establecidas sobre auditorías externas de TI.*

1. Plazos para la remisión del perfil tecnológico

a) *Para las entidades y empresas supervisadas por SUGEF, SUGEVAL y SUPEN*

i. *Plazo:*

El perfil tecnológico será remitido en los meses de febrero, mayo y agosto, según la distribución de entidades que comunique cada Superintendencia por medio de los canales oficiales de comunicación.

ii. *Canales de remisión:*

El perfil tecnológico será remitido mediante archivos XML, a través del sistema SICVECA.

iii. *Contenido y guías:*

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.

b) Para entidades y empresas supervisadas por SUGESE

i. Plazo:

El perfil tecnológico será remitido contra requerimiento expreso de SUGESE en un plazo no mayor a veinte días hábiles contados a partir de la solicitud.

ii. Canales de remisión:

El perfil tecnológico será remitido mediante archivos en Excel, a través de los canales oficiales de comunicación.

iii. Contenido y guías:

El contenido del perfil tecnológico y la guía para la descarga, llenado y remisión vigentes se encuentran en el sitio electrónico oficial de SUGESE.

2. Estudio técnico

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.

a) El estudio técnico para la debida fundamentación de los procesos de evaluación del marco de gobierno y gestión de TI que no les aplican a las entidades o empresas supervisadas contendrá:

i. Carátula del estudio.

ii. Antecedentes.

iii. Método de trabajo:

Descripción del método de trabajo.

iv. Marco de gobierno y gestión de TI:

a) Criterios para la evaluación de la aplicabilidad de los procesos que 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:

i. Estrategia.

ii. Metas.

iii. Perfil de Riesgo.

iv. Temas relacionados con TI.

v. Panorama de amenazas.

vi. Requerimientos de cumplimiento.

vii. *Rol de TI.*

viii. *Modelo de Aprovisionamiento de TI.*

ix. *Métodos de Implementación de TI.*

x. *Estrategia de Implementación de TI.*

xi. *Tamaño de la organización.*

xii. *Cualquier otro factor que se considere relevante.*

3. *Consideraciones de la naturaleza, tamaño, volumen de operaciones, modelo de negocio y riesgos de la entidad o empresa supervisada para la no adopción de los procesos*

b) *Análisis de la selección de los procesos de evaluación del marco de gobierno y de gestión de TI.*

v. *Conclusiones y recomendaciones de implementación o exclusión.*

3. Plazos y canales de comunicación de los cambios significativos del perfil tecnológico

a) Para las entidades y empresas supervisadas por SUGEF, SUGEVAL y SUPEN

i. Plazo:

La comunicación de los cambios significativos del perfil tecnológico será remitida en los meses de febrero, mayo y agosto, según la distribución de entidades que comunique cada Superintendencia por medio de los canales oficiales de comunicación.

ii. Canales:

Los cambios significativos del perfil tecnológico serán comunicados mediante el formulario de justificaciones del perfil tecnológico.

b) Para entidades y empresas supervisadas por SUGESE

i. Plazo:

La comunicación de los cambios significativos del perfil tecnológico será remitida en los meses de febrero, mayo y agosto, según la distribución de entidades que comunique la Superintendencia.

ii. Canales:

Los cambios significativos del perfil tecnológico serán comunicados mediante un documento comprensivo de cambios. La entidad o empresa supervisada definirá el formato de dicho documento de conformidad con los cambios identificados.

4. Plazo para las auditorías externas de TI

a) Una vez que las Superintendencias han comunicado el alcance de la auditoría externa de TI, las entidades y empresas supervisadas cuentan con un plazo no mayor de nueve meses para la contratación, 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.

b) Las Superintendencias podrán requerir un plazo menor de acuerdo con la definición de riesgo que represente la entidad o empresa supervisada.

5. Canales de remisión del alcance de la auditoría externa de TI

El comunicado del alcance de la auditoría será remitido a las entidades y empresas supervisadas por medio de los canales oficiales de comunicación de cada Superintendencia.

6. Formato para la planificación del encargo, así como el plazo y los canales para la remisión de la documentación del contrato y la planificación del encargo de la auditoría externa de TI

a) Formato de la planificación del encargo de la auditoría externa de TI:

i. Carátula del plan:

1. Nombre de la entidad o empresa supervisada.

2. Nombre de las Superintendencias que recibirán los resultados de la auditoría externa de TI.

3. Título: "Planificación del encargo de TI".

4. Número de referencia del oficio o requerimiento en que el supervisor de la entidad o empresa supervisada solicita la auditoría.

5. Nombre del auditor (firma, socio responsable y encargado del equipo o auditor externo independiente) y el correspondiente código del certificado CISA.

6. Nombre y puesto del aprobador del plan en la entidad o empresa supervisada.

7. Fecha de aprobación.

ii. Plan de trabajo:

1. Áreas que serán auditadas.

2. Tipo de trabajo planificado.

3. Objetivos de alto nivel y alcance del trabajo.

4. *Entrevistas de descubrimiento por realizar.*
5. *Información relevante por obtener.*
6. *Procedimientos para verificar o validar la información obtenida y su uso como evidencia de auditoría.*
7. *Temas generales, tales como:*
    i. *Presupuesto.*
    ii. *Disponibilidad y asignación de recursos.*
    iii. *Fechas de programación (cronograma detallado hasta un tercer nivel del EDT).*
    iv. *Tipo de informe.*
    v. *Público objetivo.*
    vi. *Entregables.*
8. *Temas específicos, como:*
    i. *Identificación de las herramientas necesarias para recopilar evidencia, realizar pruebas y preparar o resumir información para la generación de los informes.*
    ii. *Criterios de valoración (políticas, procedimientos o protocolo) que se usarán al evaluar las prácticas actuales.*
    iii. *Documentación de valoración de riesgos.*
    iv. *Requerimientos para la generación de informes y distribución.*
    v. *Informes externos disponibles.*

7. Plazo y canales para la remisión del contrato y la planificación del encargo de la auditoría externa de TI

El contrato y la planificación del encargo de la auditoría externa de TI serán remitidos mediante los canales oficiales de comunicación de cada Superintendencia y en un plazo máximo de treinta días hábiles contados a partir de la suscripción del contrato de la auditoría externa.

8. Formatos, contenido y canales de remisión de los productos de la auditoría externa de TI

a) El formato y contenido de los productos de la auditoría externa de TI se detallan a continuación:

1. Informe de la auditoría externa de TI

El informe de auditoría externa de TI estará foliado y contendrá lo siguiente:

1. *Carátula del informe:*
   a. *Nombre de la entidad o empresa supervisada.*
   b. *Nombre de las Superintendencias que recibirán los resultados de la auditoría externa de TI.*
   c. *Título del informe: "Auditoría externa de TI".*
   d. *Número de referencia del oficio o requerimiento en que el supervisor de la entidad o empresa supervisada solicita la auditoría.*
   e. *Nombre del auditor (firma, socio responsable y encargado del equipo o auditor externo independiente) y el correspondiente código del certificado CISA.*
   f. *Fecha de finalización del informe.*

2. *Secciones del informe:*
   a. *Generalidades de la auditoría externa:*
      i. *Identificación de la entidad o empresa supervisada:*
         1. *Tipo de entidad o empresa supervisada (entidad individual o grupo de entidades).*
         2. *Tipo de gestión de TI (individual o corporativa).*
         3. *Otros aspectos importantes a criterio del auditor.*
      ii. *Restricciones:*

      Indicar las restricciones con respecto a la circulación del informe.
      iii. *Equipo de auditoría:*

      Integración del equipo de auditoría:
         a. *Nombre completo.*
         b. *Rol dentro del equipo.*
      iv. *Período de ejecución de la auditoría:*

      Período auditado.
   b. *Alcance de la auditoría:*

   Detalle del alcance de la auditoría.

c. *Método de trabajo:*

Descripción del método de trabajo utilizado en el proceso de revisión.

d. *Limitaciones generales:*

Indicar las limitaciones generales a las que estuvo sujeta la auditoría.

e. *Resultados de la auditoría:*

i. *Opinión general.*

ii. *Conclusiones.*

iii. *Para cada proceso evaluado se requiere indicar lo siguiente:*

1. *Los hallazgos, los cuales indiquen: la condición, criterio, causa, efecto. Cuando corresponda: riesgo y recomendación por cada hallazgo.*

2. *Los escenarios de riesgos de TI de los hallazgos señalados en el punto anterior, que detallen: el actor que genera la amenaza, el tipo de amenaza, el evento o acción, los activos o recursos relacionados y la duración, cuando corresponda.*

3. *Las recomendaciones para mitigar los riesgos de TI señalados en los puntos anteriores.*

iv. *Comentarios de la gerencia al borrador de informe (documento formal y firmado que contiene los comentarios de la gerencia sobre los hallazgos y su aceptación o rechazo).*

v. *Detalle de cualquier reserva que el auditor externo de TI tuviese en cuanto al alcance de la auditoría.*

f. *Firmas:*

El informe estará firmado, al menos, por el socio responsable o auditor CISA responsable o el auditor externo independiente.

g. *Anexos:*

El informe contendrá como mínimo los siguientes anexos:

1. *Matriz de calificación del gobierno y de la gestión de TI (de la entidad o empresa supervisada y, cuando corresponda, de los proveedores de bienes y servicios de TI).*

2. *Número y fecha del acuerdo del Órgano de Dirección en el cual se aprobó el informe final de la auditoría externa de TI.*

3. *Índice de documentación de los papeles de trabajo referenciados en el informe de auditoría externa de TI y en la matriz de evaluación del gobierno y la gestión de TI con explicaciones detalladas de los documentos.*

4. *Cualquier otra información o documento considerado necesario por el auditor externo de TI.*

2. Matriz de evaluación

Las Superintendencias pondrán a disposición de las entidades y empresas supervisadas, así como de los auditores externos de TI, la versión vigente de la herramienta que contiene la Matriz de evaluación del marco de gobierno y gestión de TI, así como las respectivas guías para su uso a través de los sitios electrónicos oficiales de cada Superintendencia. Las "prácticas de gobierno y gestión" establecidas en la matriz de evaluación serán adoptadas y adaptadas por las entidades y empresas supervisadas de conformidad con sus riesgos identificados.

b) Canales de remisión de los productos de la auditoría externa de TI:

Los productos de la auditoría externa de TI serán remitidos través de los canales oficiales de comunicación de cada Superintendencia.

9. Canales de coordinación de la reunión para la presentación de los resultados de la auditoría externa de TI

La coordinación de la reunión para la presentación de los resultados de la auditoría externa de TI por parte de las entidades o empresas supervisadas se realizará por medio de los canales oficiales de comunicación de cada Superintendencia.

10. Contenido mínimo de la presentación de los resultados de la auditoría externa de TI

Contenido mínimo de la presentación de los resultados de la auditoría externa de TI:

i. Objetivos de la auditoría:

ii. Método utilizado en el proceso de revisión.

iii. Alcance de la auditoría.

iv. Período auditado.

v. Periodo de ejecución de la auditoría.

vi. Hallazgos relevantes por proceso o aspecto evaluado.

vii. Riesgos de TI relevantes.

viii. Opinión general.

ix. Recomendaciones.

11. Personas que se requiere que asistan a la presentación de los resultados de la auditoría externa de TI:

a) El presidente del Órgano de Dirección o el directivo que se encuentra destacado en el Comité de TI de las entidades y empresas supervisadas.

b) El gerente general o el representante legal de las entidades o empresas supervisadas.

c) El responsable de la unidad de TI, o similar, de las entidades y empresas supervisadas.

d) El auditor interno de las entidades y empresas supervisadas.

e) El presidente del comité de vigilancia, cuando exista dicho cargo en las entidades y empresas supervisadas.

f) El responsable de la función, unidad o funciones equivalentes de seguridad de la información y seguridad cibernética de las entidades o empresas supervisadas cuando se evalúen controles sobre dicha área.

12. Plan de acción para la atención de los hallazgos de la auditoría externa de TI

a) Los aspectos que se considerarán en la elaboración del plan de acción para la atención de los hallazgos de la auditoría externa de TI son los siguientes:

i. Las Superintendencias pondrán a disposición de las entidades y empresas supervisadas y de los auditores externos de TI, la versión vigente del "Plan de acción para la atención de los hallazgos de la auditoría externa de TI", así como la respectiva "Guía para la descarga, llenado y remisión del plan de acción" a través de los sitios electrónicos oficiales de cada Superintendencia.

ii. Los planes de acción para la atención de los hallazgos de la auditoría externa de TI especificarán claramente la acción a implementar, su duración o plazo de ejecución, las fechas de inicio y fin de ejecución, el porcentaje de avance, el responsable, los indicadores para medir la efectividad de las acciones tomadas para mitigar el riesgo o corregir el hallazgo y una explicación clara de cómo las acciones van a lograr lo propuesto.

iii. El plan de acción incluirá la frecuencia de presentación de informes de avance con plazos no mayores a seis meses.

iv. *El plan de acción estará firmado por el representante legal de la entidad o empresa supervisada.*

v. *En caso de que el supervisor lo requiera, las entidades o empresas supervisadas ejecutarán modificaciones en el plan de acción. El plan de acción con las modificaciones será aprobado por el Órgano de Dirección, estará firmado por el representante legal de la entidad o empresa supervisada y será comunicado, nuevamente, al supervisor en el plazo requerido por este.*

Sección XIV. Lineamientos relacionados con las pautas para la elaboración de las solicitudes de prórroga para el plazo de la remisión de los productos de la auditoría externa de TI y el plazo de la remisión del plan de acción, así como los canales de remisión de las solicitudes

***Objetivo**: Establecer las pautas para la elaboración de las solicitudes de prórroga para el plazo de la remisión de los productos de la auditoría externa de TI y el plazo de la remisión del plan de acción, así como los canales de remisión de las solicitudes.*

1. *Las pautas para considerar en la elaboración de las solicitudes de prórroga son las siguientes:*

   a) *La solicitud será suscrita por el representante legal de la entidad o empresa supervisada.*

   b) *Indicar la fecha propuesta de remisión de los productos de la auditoría externa de TI o acompañarse de un nuevo plan de acción aprobado por su Órgano de Dirección, según corresponda.*

   c) *Indicar los motivos y las pruebas, si fuere el caso, que imposibilitan a la entidad o empresa supervisada cumplir con el plazo original y demostrar que los motivos para su petición se basan en caso fortuito o fuerza mayor u otras causas fuera de su control.*

2. *Canales de remisión de las solicitudes de prórroga:*

   a) *Para las solicitudes de prórroga se elaborará un oficio, el cual, será remitido mediante los canales oficiales de comunicación de cada Superintendencia.*

Sección XV. Anexos

Anexo 1

Procesos de evaluación del marco de gobierno y gestión de TI

1. Procesos de evaluación del gobierno de TI

ID	*Aspectos del marco de gobierno de TI*	*Descripción*	*Propósito*
1.01	*Asegurar el establecimiento y el mantenimiento del marco de gobierno*	*Analizar y articular los requisitos para el gobierno de la tecnología de información de la entidad o empresa supervisada. Establecer y mantener componentes de gobierno claros con respecto a la autoridad y las responsabilidades para lograr la misión, las metas y los objetivos de la entidad o empresa supervisada.*	*Proporcionar un enfoque consistente integrado y alineado con el enfoque de gobierno de la entidad o empresa supervisada. Las decisiones relacionadas con información y las tecnologías deben hacerse en línea con las estrategias y objetivos de la entidad o empresa supervisada y para alcanzar el valor deseado. En este sentido, debe asegurarse de que los procesos relacionados con la información y las tecnologías se supervisen de forma eficaz y transparente; que se cumpla con los requisitos legales, contractuales y regulatorios; y que se cumplan los requisitos de gobierno para los miembros del Órgano de Dirección.*
1.02	*Asegurar la obtención de beneficios*	*Optimizar el valor al negocio de las inversiones en procesos de la entidad o empresa supervisada, servicios y activos de información y tecnológicos.*	*Asegurar un valor óptimo de las iniciativas, servicios y activos habilitados para información y las tecnologías; la entrega rentable de soluciones y servicios; así como una imagen confiable y precisa de los costes y beneficios probables para que las necesidades de la entidad o empresa supervisada se satisfagan de forma eficaz y eficiente.*
1.03	*Asegurar la optimización del riesgo*	*Asegurar que el apetito ~~y~~, la tolerancia y la capacidad al riesgo de la entidad o empresa supervisada se entiendan, articulen y comuniquen, además, que se identifique y gestione el riesgo para el valor de negocio relacionado con el uso de la tecnología de información.*	*Asegurarse de que el riesgo de negocio relacionado con la información y las tecnologías no exceda el apetito, tolerancia y capacidad al riesgo de la entidad o empresa supervisada, que se identifique y gestione el impacto del riesgo relacionados y generados con la información y las tecnologías para el valor de negocio y que se minimicen los posibles fallos de cumplimiento.*
1.04	*Asegurar la optimización de los recursos*	*Asegurar que se dispone de recursos adecuados y suficientes relacionados con la información y las tecnologías (personas, procesos y tecnología), así como con el negocio para apoyar eficazmente los objetivos de la entidad o empresa supervisada, a un coste óptimo.*	*Asegurarse de que las necesidades de recursos de la entidad o empresa supervisada se satisfagan de manera óptima, que los costes de la tecnología de información se optimicen, y que exista una mayor probabilidad de obtener beneficios y disponibilidad para cambios futuros.*
1.05	*Asegurar el compromiso de las partes interesadas*	*Asegurar que se identifica e involucra a las partes interesadas en el sistema de gobierno de la tecnología de información y que la medición y comunicación sobre el rendimiento, su conformidad en la entidad o empresa supervisada sean transparentes, con las partes interesadas aprobando las metas, métricas y las acciones remediales necesarias.*	*Asegurarse de que las partes interesadas apoyen la estrategia y la hoja de ruta de la tecnología de información, que la comunicación con las partes interesadas sea eficaz y oportuna, y que se establezcan las bases para los informes con el fin de aumentar el rendimiento. Identificar las áreas de mejora y confirmar que sus objetivos y estrategias relacionadas se ajusten a la estrategia de la entidad o empresa supervisada.*

2. Procesos de evaluación de la gestión de TI

ID	Aspectos del marco de gestión de TI	Descripción	Propósito
2.01	Gestionar el marco de gestión de información y las tecnologías.	Diseñar el sistema de gestión para la información y las tecnologías de la entidad o empresa supervisada basándose en las metas de la entidad o empresa supervisada y otros factores de diseño. Con base en este diseño, implementar todos los componentes necesarios del sistema de gestión.	Implementar un enfoque de gestión consistente para permitir que se alcancen los requisitos de gobierno organizacional, con cobertura de componentes de gobierno, como los procesos de gestión, las estructuras organizativas, los roles y las responsabilidades, las actividades confiables y repetibles, los elementos de información, las políticas y procedimientos, las habilidades y las competencias, la cultura y el comportamiento, así como los servicios, infraestructura y aplicaciones.
2.02	Gestionar la estrategia.	Proporcionar una visión holística del entorno organizacional y de información y las tecnologías actuales, la dirección futura y las iniciativas necesarias para migrar al entorno futuro deseado. Garantizar que el nivel de digitalización deseado sea integral en la dirección y la estrategia de la tecnología de información futuras. Evaluar la madurez digital actual de la entidad o empresa supervisada y desarrollar una hoja de ruta para reducir las brechas. Repensar, con la entidad o empresa supervisada, las operaciones internas, así como las actividades de cara al cliente. Garantizar el alcance en la ruta de transformación a través de toda la entidad o empresa supervisada. Aprovechar los bloques de construcción de la arquitectura organizacional, los componentes del gobierno y el ecosistema de la entidad o empresa supervisada, incluyendo servicios y capacidades relacionadas que se proporcionan externamente, para permitir una respuesta confiable, también ágil y eficiente a los objetivos estratégicos.	Apoyar la estrategia de transformación digital de la entidad o empresa supervisada y proporcionar el valor deseado a través de una hoja de ruta con cambios incrementales. Usar un enfoque holístico en cuanto a la información y las tecnologías, asegurando que cada iniciativa esté claramente conectada con una estrategia global. Habilitar el cambio en todos los diversos aspectos de la entidad o empresa supervisada, desde los canales y procesos hasta los datos, cultura, habilidades, modelo operativo e incentivos.
2.03	Gestionar la arquitectura organizacional.	Establecer una arquitectura común que consiste en capas de arquitectura de procesos de negocio, información, datos, aplicaciones y tecnología. Crear modelos y prácticas claves que describen las arquitecturas base y objetivo, en línea con la estrategia de tecnologías e información de la entidad o empresa supervisada. Definir los requisitos de taxonomía, estándares, directrices, procedimientos, plantillas y herramientas, y proporcionar un vínculo para estos componentes. Mejorar el alineamiento, aumentar la agilidad, mejorar la calidad de la información y generar ahorros potenciales de costes mediante iniciativas como la reutilización de componentes de bloques de construcción.	Representar los diferentes bloques de construcción que conforman la entidad o empresa supervisada y sus interrelaciones, así como los principios que guían su diseño y evolución a lo largo del tiempo, para posibilitar una prestación estándar, responsable y eficiente de los objetivos operativos y estratégicos.
2.04	Gestionar la innovación.	Mantener una concienciación de tecnología e información y tendencias de servicio relacionadas, así como monitorizar las tendencias tecnológicas emergentes. Identificar de forma proactiva oportunidades de innovación y planificar cómo beneficiarse de la innovación en relación con las necesidades organizacionales y la estrategia de tecnología e información. Analizar qué oportunidades de mejora o innovación organizacional pueden crearse mediante tecnologías emergentes, servicios o innovación organizacional habilitada por tecnología e información, así como a través de	Lograr ventajas competitivas, innovación organizacional, una mejor experiencia del cliente y una mayor eficacia y eficiencia operativa con el aprovechamiento de los desarrollos de tecnología e información y tecnologías emergentes.

ID	Aspectos del marco de gestión de TI	Descripción	Propósito
		tecnologías ya establecidas y por la innovación de procesos organizacionales y de TI. Influenciar la planificación estratégica y las decisiones de arquitectura organizacional.	
2.05	*Gestionar el portafolio.*	*Ejecutar la dirección estratégica establecida para las inversiones, en línea con la visión de la arquitectura organizacional y la hoja de ruta de tecnología e información. Considerar las diferentes categorías de inversiones y las limitaciones de recursos y financiación. Evaluar, priorizar y equilibrar los programas y servicios, gestionando la demanda dentro de las limitaciones de recursos y financiamiento, basándose en su alineación con los objetivos estratégicos, el valor y el riesgo de la entidad o empresa supervisada. Mover los programas seleccionados al portafolio de productos o servicios activo para su ejecución. Supervisar el rendimiento del portafolio general de productos y servicios, y programas, proponiendo ajustes según sea necesario en respuesta al rendimiento del programa, producto o servicio, o cambiando las prioridades de la entidad o empresa supervisada.*	*Optimizar el rendimiento del portafolio general de programas en respuesta al rendimiento individual de programas, productos y servicios, así como a las cambiantes prioridades y demandas de la entidad o empresa supervisada.*
2.06	*Gestionar el presupuesto y los costes.*	*Gestionar las actividades financieras relacionadas con tecnología e información en las funciones organizacionales y de TI, cubriendo el presupuesto, la gestión de costes y beneficios, así como la priorización de gastos mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de asignación de costes a la entidad o empresa supervisada. Consultar a las partes interesadas para identificar y controlar los costes y beneficios totales dentro del contexto de los planes estratégicos y tácticos de tecnología e información. Iniciar la acción correctiva cuando sea necesario.*	*Fomentar la asociación entre las partes interesadas de la entidad o empresa supervisada y de TI para permitir el uso eficaz y eficiente de los recursos relacionados con tecnología e información, y proporcionar transparencia y rendición de cuentas sobre el coste y el valor para el negocio de soluciones y servicios. Habilitar a la entidad o empresa supervisada para que tome decisiones informadas sobre el uso de soluciones y servicios de tecnología e información.*
2.07	*Gestionar los recursos humanos.*	*Proporcionar un enfoque estructurado para asegurar una contratación/adquisición, planificación, evaluación y desarrollo de recursos humanos óptimos (tanto interna como externamente).*	*Optimizar las capacidades de recursos humanos para satisfacer los objetivos de la entidad o empresa supervisada.*
2.08	*Gestionar las relaciones.*	*Gestionar las relaciones con las partes interesadas de una manera formal y transparente que asegure una confianza mutua y un enfoque combinado en lograr las metas estratégicas dentro de las limitaciones de los presupuestos y la tolerancia al riesgo. Basar las relaciones de la comunicación abierta y transparente, un lenguaje común, así como la voluntad de responsabilizarse y rendir cuentas por las decisiones clave por ambas partes. La entidad o empresa supervisada y TI deben trabajar juntos para generar resultados organizacionales exitosos que respalden los objetivos organizacionales.*	*Facilitar el conocimiento, habilidades y comportamientos correctos para generar mejores resultados, aumentar la confianza, credibilidad mutua y uso eficaz de los recursos, a fin de estimular una relación productiva con las partes interesadas de la entidad o empresa supervisada.*
2.09	*Gestionar los acuerdos de servicio.*	*Alinear los productos y servicios habilitados por tecnología e información y los niveles de servicio con las necesidades y expectativas de la empresa, incluidos la identificación, especificación, diseño, publicación, acuerdo y monitorización de los productos y servicios de tecnología e*	*Asegurarse de que los productos, servicios y niveles de servicio de tecnología e información satisfagan las necesidades actuales y futuras de la entidad o empresa supervisada.*

ID	Aspectos del marco de gestión de TI	Descripción	Propósito
		información, niveles de servicio e indicadores de rendimiento.	
2.10	*Gestionar los proveedores.*	*Gestionar los productos y servicios relacionados con tecnología e información proporcionados por todo tipo de proveedores para que satisfagan los requisitos de la entidad o empresa supervisada. Esto incluye la búsqueda y selección de proveedores, gestión de relaciones, gestión de contratos, además, revisión y monitorización del rendimiento de proveedores y el ecosistema de proveedores (incluida la cadena ascendente de suministro) para que sea efectiva y cumpla con la legislación.*	*Optimizar las capacidades de tecnología e información disponibles para apoyar la estrategia y la hoja de ruta, minimizar el riesgo asociado con proveedores que no rinden o cumplen con los requisitos y asegurar precios competitivos.*
2.11	*Gestionar la calidad.*	*Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados organizacionales relacionados. Habilitar los controles, monitorización continua y uso de prácticas y estándares probados en esfuerzos de mejora y eficiencia continuos.*	*Asegurar la prestación consistente de soluciones y servicios de TI para satisfacer los requisitos de calidad de la entidad o empresa supervisada y las necesidades de las partes interesadas.*
2.12	*Gestionar el riesgo.*	*Identificar, evaluar y reducir continuamente los riesgos relacionados con tecnología e información dentro de los niveles de tolerancia establecidos por la entidad o empresa supervisada.*	*Integrar la gestión del riesgo organizacional relacionado con la tecnología e información, con la gestión del riesgo organizacional global y equilibrar los costes y beneficios de la gestión del riesgo organizacional relacionado con las tecnología e información.*
2.13	*Gestionar la seguridad.*	*Definir, operar y monitorizar un sistema de gestión de seguridad de la información.*	*Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la entidad o empresa supervisada.*
2.14	*Gestionar los datos.*	*Lograr y mantener la gestión eficaz de los activos de datos de la entidad o empresa supervisada durante todo el ciclo de vida de los datos, desde la creación hasta su entrega, mantenimiento y archivo.*	*Garantizar el uso eficaz de activos de datos críticos para lograr las metas y objetivos organizacionales.*
2.15	*Gestionar los programas*	*Gestionar todos los programas del portafolio de inversión, de conformidad con la estrategia de la entidad o empresa supervisada y de forma coordinada, según un enfoque de gestión de programas estándar. Iniciar, planificar, controlar y ejecutar programas, así como monitorizar el valor esperado del programa.*	*Obtener el valor de negocio deseado y reducir el riesgo de retrasos, costes y erosión de valor inesperados. Para ello, mejorar las comunicaciones y la participación del negocio y usuarios finales, garantizar el valor y la calidad de los entregables del programa; realizar un seguimiento de los proyectos dentro de los programas, además, maximizar la contribución del programa al portafolio de inversiones.*
2.16	*Gestionar la definición de requisitos*	*Identificar las soluciones y analizar los requisitos antes de su adquisición o construcción para asegurarse de que se ajustan a los requisitos estratégicos de la empresa cubriendo los procesos, aplicaciones, información/datos, infraestructura y servicios del negocio Coordinar la revisión de opciones viables con las partes interesadas afectadas, incluidos costes y beneficios relativos, análisis de riesgos, aprobación de los requisitos y soluciones propuestas.*	*Crear soluciones óptimas que satisfagan las necesidades de la entidad o empresa supervisada mientras que se minimiza el riesgo.*
2.17	*Gestionar la identificación y construcción de soluciones*	*Establecer y mantener productos y servicios identificados (tecnología, procesos de negocio y flujos de trabajo) alineados con los requisitos de la entidad o empresa supervisada que cubran el diseño, desarrollo, adquisición/subcontratación y la asociación con proveedores. Gestionar la configuración, preparación de pruebas, pruebas, gestión de requisitos y mantenimiento de*	*Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la entidad o empresa supervisada.*

ID	Aspectos del marco de gestión de TI	Descripción	Propósito
		procesos de negocio, aplicaciones, información/datos, infraestructura y servicios.	
2.18	*Gestionar la disponibilidad y la capacidad*	*Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con la prestación de servicios rentables. Incluir la evaluación de las capacidades actuales, previsión de las necesidades futuras basándose en los requisitos del negocio, el análisis de impactos en el negocio y la evaluación del riesgo, para planificar e implementar acciones que satisfagan los requisitos identificados.*	*Mantener la disponibilidad del servicio, la gestión eficiente de los recursos y la optimización del rendimiento del sistema a través de la predicción de los requisitos futuros de rendimiento y capacidad.*
2.19	*Gestionar el cambio organizativo*	*Maximizar la probabilidad de implementar con éxito un cambio organizativo sostenible en toda la entidad o empresa supervisada, de forma rápida y con un riesgo reducido. Cubrir el ciclo de vida completo del cambio y todas las partes interesadas en el negocio y en TI.*	*Preparar y conseguir el compromiso de las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.*
2.20	*Gestionar los cambios de TI*	*Gestionar todos los cambios de una manera controlada, incluidos los cambios estándar y los mantenimientos de emergencia en relación con los procesos de negocio, las aplicaciones y la infraestructura. Esto incluye estándares y procedimientos de cambio, evaluación del impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación.*	*Facilitar una ejecución de cambios rápida y confiable para el negocio. Mitigar el riesgo de afectar negativamente la estabilidad o integridad del entorno que se ha modificado.*
2.21	*Gestionar la aceptación y transición de los cambios de TI*	*Aceptar formalmente y hacer operativas las nuevas soluciones. Incluir la planificación de la implementación, conversión de sistemas y datos, pruebas de aceptación, comunicación, preparación de la puesta en producción, paso a producción de nuevos o modificados procesos de negocio y servicios de tecnología e información, soporte temprano de la producción y revisión posterior a la implementación.*	*Implementar soluciones de forma segura y conforme a las expectativas y resultados acordados.*
2.22	*Gestionar el conocimiento*	*Mantener disponible la información de gestión relevante, vigente, conocimiento validado y confiable con el fin de apoyar todas las actividades del proceso y facilitar la toma de decisiones relacionadas con el gobierno y la gestión de tecnología e información de la empresa. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada del conocimiento.*	*Proporcionar el conocimiento e información de gestión necesarios para apoyar a todo el personal en el gobierno y gestión de la tecnología e información de la entidad o empresa supervisada y facilitar la toma de decisiones informada.*
2.23	*Gestionar los activos*	*Gestionar los activos de tecnología e información a través de su ciclo de vida para asegurarse de que su uso aporta valor a un coste óptimo, continúan operativos (adecuados a su propósito), se tienen en cuenta y están físicamente protegidos. Asegurar que aquellos activos que son críticos para soportar la capacidad del servicio son confiables y están disponibles. Gestionar las licencias de software para asegurarse de que se adquiere, retiene y despliega la cantidad óptima en relación con el uso que requiere el negocio, y que el software instalado cumpla con los acuerdos de licencia.*	*Tener en cuenta todos los activos de tecnología e información y optimizar el valor proporcionado por su uso.*
2.24	*Gestionar la configuración*	*Definir y mantener descripciones y relaciones entre recursos claves y las capacidades necesarias para ofrecer servicios habilitados por tecnología e información. Incluir la recopilación de información sobre la configuración, estableciendo líneas de referencia, verificando y*	*Proporcionar información suficiente sobre los activos de servicio para facilitar que el servicio se gestione de forma eficiente. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.*

ID	Aspectos del marco de gestión de TI	Descripción	Propósito
		auditando esta información, y actualizando el repositorio de configuración	
2.25	*Gestionar los proyectos*	*Gestionar todos los proyectos que se inician en la entidad o empresa supervisada, alineados con la estrategia organizacional y de forma coordinada, con base en una estrategia de gestión de proyectos estándar. Iniciar, planificar, controlar y ejecutar proyectos, así como concluir con una revisión post-implementación.*	*Lograr los resultados definidos en el proyecto y reducir el riesgo de retrasos inesperados, costes y erosión del valor mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Garantizar el valor y la calidad de los entregables del proyecto y maximizar su contribución a los programas definidos y al portafolio de inversiones.*
2.26	*Gestionar las operaciones*	*Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de tecnología e información internos y tercerizados. Incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas.*	*Proporcionar los resultados de los productos y servicios operativos de tecnología e información según lo planeado.*
2.27	*Gestionar las peticiones y los incidentes del servicio*	*Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restaurar el servicio normal, registrar y completar las solicitudes de usuario; así como registrar, investigar, diagnosticar, escalar y resolver los incidentes. (Incluyen, entre otros, los incidentes de seguridad de la información y de seguridad cibernética)*	*Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes. (Incluyen entre otros, los incidentes de seguridad de la información y de seguridad cibernética)*
2.28	*Gestionar los problemas*	*Identificar y clasificar los problemas y su causa raíz. Ofrecer una solución oportuna para evitar incidentes recurrentes. Ofrecer recomendaciones de mejoras.*	*Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente, así como lograr su satisfacción mediante una reducción del número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas.*
2.29	*Gestionar la continuidad*	*Establecer y mantener un plan que permita a las organizaciones y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones. Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de tecnología e información necesarios, además, mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la entidad o empresa supervisada.*	*Adaptarse rápidamente, continuar con las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la entidad o empresa supervisada en caso de una interrupción significativa (p.ej., amenazas, oportunidades, demandas).*
2.30	*Gestionar los servicios de seguridad*	*Proteger la información de la entidad o empresa supervisada para mantener el nivel de riesgo de la seguridad de la información aceptable para la entidad o empresa supervisada, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad.*	*Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información.*
2.31	*Gestionar los controles de los procesos de negocio*	*Definir y mantener los controles apropiados de los procesos de negocio para asegurar que la información relacionada y procesada por procesos de negocio internos o tercerizados cumpla con todos los requisitos relevantes de control de la información. Identificar los requisitos relevantes de control de la información. Gestionar y operar los controles adecuados de entrada, throughput y salida (controles de aplicación) para asegurar que la información y el procesamiento de la información cumpla con estos requisitos.*	*Mantener la integridad de la información y la seguridad de los activos de información manejados dentro de los procesos de negocio, dentro de la entidad o empresa supervisada u operación tercerizada.*
2.32	*Gestionar la monitorización del*	*Recopilar, validar y evaluar las metas y métricas de alineamiento de la entidad o empresa*	*Proporcionar transparencia en el rendimiento y la conformidad e impulsar la consecución de las metas.*

ID	Aspectos del marco de gestión de TI	Descripción	Propósito
	rendimiento y la conformidad	*supervisada. Supervisar que los procesos y las prácticas se desempeñen según las metas y métricas de rendimiento y conformidad acordadas. Proporcionar informes sistemáticos y oportunos.*	
2.33	*Gestionar el sistema de control interno*	*Supervisar y evaluar continuamente el entorno de control, incluyendo autoevaluaciones y autoconcienciación. Habilitar a la gerencia para identificar deficiencias e ineficiencias de control e iniciar acciones de mejora. Planificar, organizar y mantener estándares para la evaluación del control interno y la eficacia del control de procesos.*	*Dar información transparente a las partes interesadas clave sobre la idoneidad del sistema de controles internos que permita proporcionar confianza en las operaciones, confianza en el logro de los objetivos de la entidad o empresa supervisada y una comprensión adecuada del riesgo residual.*
2.34	*Gestionar el cumplimiento de los requisitos externos*	*Evaluar si los procesos de tecnología e información y los procesos de negocio apoyados por tecnología e información cumplen con las leyes, regulaciones y requisitos contractuales. Asegurar que los requisitos se han identificado y cumplido; integrar el cumplimiento de TI con el cumplimiento general de la entidad o empresa supervisada.*	*Asegurarse de que la entidad o empresa supervisada cumpla con todos los requisitos externos aplicables.*
2.35	*Gestionar el aseguramiento*	*Planificar, delimitar y ejecutar iniciativas de aseguramiento para cumplir con requisitos internos, leyes, regulaciones y objetivos estratégicos. Permitir que la dirección ofrezca una garantía adecuada y sostenible en la entidad o empresa supervisada, con la realización de revisiones y actividades de aseguramiento independiente.*	*Facilitar a la entidad o empresa supervisada el diseño y desarrollo de iniciativas de aseguramiento eficaces y eficientes proporcionando una guía sobre la planificación, alcance, ejecución y seguimiento de las revisiones de aseguramiento con una hoja de ruta basada en estrategias de aseguramiento ampliamente aceptadas.*

Anexo 2

Procesos de evaluación de la gestión de TI para la regulación proporcional

1. ***Procesos de evaluación de la gestión de TI para entidades supervisadas por SUGEF sujetas a la Regulación proporcional para cooperativas de ahorro y crédito, Acuerdo SUGEF 25-23 (la descripción de cada proceso se encuentra en el Anexo 1):***
   a. *2.01 Gestionar el marco de gestión de información y las tecnologías*
   b. *2.02 Gestionar la estrategia*
   c. *2.06 Gestionar el presupuesto y los costos*
   d. *2.09 Gestionar los acuerdos de servicio*
   e. *2.10 Gestionar los proveedores*
   f. *2.12 Gestionar el riesgo*
   g. *2.13 Gestionar la seguridad*
   h. *2.20 Gestionar los cambios de TI*
   i. *2.23 Gestionar los activos*
   j. *2.27 Gestionar las peticiones y los incidentes del servicio*
   k. *2.29 Gestionar la continuidad*
   l. *2.30 Gestionar servicios de seguridad*
   m. *2.33 Gestionar el sistema de control interno*

2. ***Procesos de evaluación de la gestión de TI para Sociedades Corredoras de Seguros (la descripción de cada proceso se encuentra en el Anexo 1):***
   a. *2.01 Gestionar el marco de gestión de información y las tecnologías*
   b. *2.09 Gestionar los acuerdos de servicio*
   c. *2.10 Gestionar los proveedores*
   d. *2.12 Gestionar el riesgo*
   e. *2.13 Gestionar la seguridad*
   f. *2.27 Gestionar las peticiones y los incidentes de servicio*
   g. *2.29 Gestionar la continuidad*
   h. *2.30 Gestionar los servicios de seguridad*
   i. *2.33 Gestionar el sistema de control interno*

Anexo 3

Criterios para la calificación de los procesos de evaluación del marco de gobierno y gestión de TI

Cada proceso de evaluación del marco de gobierno y gestión de TI será calificado en alguna de las siguientes categorías: fuerte, aceptable, mejorable o débil.

En la siguiente tabla se detallan las categorías y criterios para la calificación de los procesos de evaluación del marco de gobierno y de gestión de TI:

Categorías de calificación del proceso de evaluación	***Criterios para la calificación del proceso de evaluación***
Fuerte	*Las características de la función tales como las responsabilidades, estructura, recursos, metodologías y prácticas, superan lo que se considera necesario*, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad, y su desempeño ha sido altamente efectivo y consistente. Las características y el desempeño de la función son superiores a las mejores prácticas utilizadas por la industria.*
Aceptable	*Las características de la función, tales como las responsabilidades, estructura, recursos, metodologías y prácticas, cumplen con lo necesario*, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad y su desempeño ha sido efectivo. Las características y el desempeño de la función cumplen con las mejores prácticas utilizadas por la industria.*
Mejorable	*Las características de la función, tales como las responsabilidades, estructura, recursos, metodologías y prácticas, generalmente cumplen con lo necesario*, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad. El desempeño de la función ha sido generalmente efectivo, pero existen áreas que necesitan mejoras. Esas mejoras no son suficientemente relevantes como para causar preocupaciones, siempre y cuando sean atendidas oportunamente. Las características y el desempeño no cumplen sistemáticamente con mejores prácticas utilizadas por la industria.*
Débil	*Las características de la función, tales como las responsabilidades, estructura, recursos, metodologías y prácticas, no cumplen de manera significativa con lo necesario*, dada la naturaleza, complejidad, importancia sistémica y perfil de riesgo de la entidad. El desempeño de la función ha demostrado serias debilidades que necesitan ser atendidas de inmediato. Las características y el desempeño frecuentemente no cumplen con las mejores prácticas utilizadas por la industria.*

**Por "necesario" se entiende: la adopción, adaptación e implementación de los procesos, prácticas y controles relacionados con el Marco de Gobierno y Gestión de TI, así como las demás disposiciones establecidas en la reglamentación vigente, que la entidad o empresa supervisada implemente para mitigar sus riesgos, que debe ser sustentado de forma cualitativa y cuantitativa."*

Anexo 4

Funciones para la evaluación de la gestión de riesgos de seguridad cibernética

Las funciones para la evaluación de la gestión de riesgos de la seguridad cibernética aplicables en el momento de la solicitud de la auditoría externa de TI son las siguientes:

1. Función Gobernar

Esta función tiene como objetivo establecer y monitorear la estrategia, expectativas y política de gestión de riesgos de seguridad cibernética de las entidades y empresas supervisadas.

ID	Categoría	Descripción
1.01	Contexto organizacional	Comprender las circunstancias (misión, expectativas de las partes interesadas y requisitos legales, regulatorios y contractuales) que rodean las decisiones de gestión de riesgos de seguridad cibernética de la entidad o empresa supervisada.
1.02	Estrategia de gestión de riesgos	Definir las prioridades, limitaciones, declaraciones de apetito y tolerancia al riesgo, así como los supuestos de la entidad o empresa supervisada que se establecen, comunican y utilizan para respaldar las decisiones de riesgo operativo.
1.03	Gestión de riesgos de la cadena de suministro de seguridad cibernética	Los procesos de gestión de riesgos de la cadena de suministro cibernético son identificados, establecidos, gestionados, monitoreados y mejorados por las partes interesadas de la entidad o empresa supervisada.
1.04	Roles, responsabilidades y autoridades	Se establecen y comunican roles, responsabilidades y autoridades de seguridad cibernética para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.
1.05	Políticas, procesos y procedimientos	Se establecen, comunican y hacen cumplir políticas, procesos y procedimientos de seguridad de la entidad o empresa supervisada.
1.06	Supervisión	Los resultados de las actividades y el desempeño de la gestión de riesgos de seguridad cibernética en toda la entidad o empresa supervisada se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.

2. Función Identificar

Esta función tiene como objetivo ayudar a determinar el riesgo de seguridad cibernética actual para las entidades y empresas supervisadas.

ID	Categoría	Descripción
2.01	Gestión de activos	Los activos de información que permiten a la entidad o empresa supervisada lograr sus propósitos comerciales se identifican y gestionan de acuerdo con su importancia relativa para sus objetivos y su estrategia de riesgo.
2.02	Evaluación de riesgos	La entidad o empresa supervisada comprende el riesgo de seguridad cibernética para la organización, los activos y el personal.
2.03	Mejora	Las mejoras en los procesos, procedimientos y actividades de gestión de riesgos de seguridad cibernética de la entidad o empresa supervisada se identifican en todas las funciones.

3. Función Proteger

Esta función tiene como objetivo establecer las salvaguardas para prevenir o reducir el riesgo de seguridad cibernética para las entidades y empresas supervisadas.

ID	Categoría	Descripción
3.01	Gestión de identidad, autenticación y control de acceso	El acceso a activos físicos y lógicos está limitado a usuarios, servicios y hardware autorizados, además, se gestiona de manera proporcional al riesgo evaluado de acceso no autorizado.
3.02	Sensibilización y formación	El personal de la entidad o empresa supervisada recibe formación y sensibilización en seguridad cibernética para que pueda realizar sus tareas relacionadas con esta.
3.03	Seguridad de datos	Los datos se gestionan de manera consistente con la estrategia de riesgo de la entidad o empresa supervisada para proteger la confidencialidad, integridad y disponibilidad de la información.
3.04	Seguridad de plataforma	El hardware, software (p. ej., firmware, sistemas operativos, aplicaciones) y servicios de plataformas físicas y virtuales se gestionan de manera consistente con la estrategia de riesgo de la entidad o empresa supervisada para proteger su confidencialidad, integridad y disponibilidad.
3.05	Resiliencia de la infraestructura tecnológica	Las arquitecturas de seguridad se gestionan con la estrategia de riesgo de la entidad o empresa supervisada para proteger la confidencialidad, integridad y disponibilidad de sus activos, y su resiliencia.

4. Función Detectar

Esta función tiene como objetivo buscar y analizar posibles ataques y compromisos de seguridad cibernética en las entidades y empresas supervisadas.

ID	Categoría	Descripción
4.01	Monitoreo continuo	Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos.
4.02	Análisis de eventos adversos	La entidad o empresa supervisada analiza anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizar los eventos y detectar incidentes de seguridad cibernética.

5. Función Responder

Esta función tiene como objetivo tomar medidas respecto a un incidente de seguridad cibernética detectado por las entidades o empresas supervisadas.

ID	Categoría	Descripción
5.01	Gestión de incidentes	La entidad o empresa supervisada gestiona las respuestas a los incidentes de seguridad cibernética detectados.
5.02	Análisis de incidentes	La entidad o empresa supervisada lleva a cabo una investigación para garantizar una respuesta efectiva y respaldar las actividades forenses y de recuperación.
5.03	Informes y comunicación de respuesta a incidentes	La entidad o empresa supervisada coordina con las partes interesadas internas y externas según lo exigen las leyes, regulaciones o políticas, las actividades de respuesta de incidentes.
5.04	Mitigación de incidentes	Las entidades o empresas supervisadas realizan actividades para prevenir la expansión de un evento y mitigar sus efectos.

6. Función Recuperar

Esta función tiene como objetivo restaurar activos de información y operaciones que se vieron afectados por un incidente de seguridad cibernética en la entidad o empresa supervisada.

ID	*Categoría*	*Descripción*
6.01	*Ejecución del Plan de Recuperación de Incidentes*	*La entidad o empresa supervisada realiza actividades de restauración para garantizar la disponibilidad operativa de los sistemas y servicios afectados por incidentes de seguridad cibernética.*
6.02	*Comunicación de recuperación de incidentes*	*La entidad o empresa supervisada coordina con partes internas y externas las actividades de restauración para la recuperación de incidentes.*

Rigen a partir de la publicación del Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24, en el diario oficial La Gaceta."

Atentamente,

Firmado Digitalmente

María del Rocío Aguilar Montoya
Superintendente General
Superintendencia General de Entidades Financieras
Superintendencia de Pensiones

Firmado Digitalmente

Tomás Soley Pérez
Superintendente General
Superintendencia General de Seguros
Superintendencia General de Valores

C. ***Asociación Costarricense de Auditores en Informática,*** *Correo electrónico: presidente@isacacr.org*
Asociación Bancaria Costarricense, *Correo electrónico: secretaria@abc.fi.cr*
Asociación de Aseguradoras Privadas de Costa Rica, *Correo electrónico: info@aap.cr*
Asociación Costarricense de Operadoras de Pensiones, *Correo electrónico: acop@acop.or.cr*
Cámara de Bancos e Instituciones Financieras de Costa Rica,
Correo electrónico: directora@camaradebancos.fi.cr ; arojas@camaradebancos.fi.cr
Cámara de Intermediarios de Seguros, *Correo electrónico: info@ciscostarica.com*
FEDEAC R.L. *Correo electrónico: milagrov@fedeac.com ; gerencia@fedeac.com*
FECOOPSE R.L. *Correo electrónico: cmontero@fecoopse.co ; xcampos@fecoopse.com*

HISTORIAL DE CAMBIOS

Versión 1: Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante artículos 8 y 9 de las actas de las sesiones 1876-2024 y 1877-2024, celebradas el 15 de julio del 2024. Rige a partir de su publicación en el diario oficial La Gaceta. Publicado en el Alcance 130 a La Gaceta 134 del 22 de julio de 2024.

Resolución SGF-2377-2024; SP-R-2236-2024, SGS-0844-2024, SGV-C03/0-1318 del 5 de agosto del 2024, por medio de la cual se modifican de forma integral los Lineamientos Generales del Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24.