Ajustes a partir de la primera consulta externa:

- Modificación integral del Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17.

- Lineamientos Generales.

CONASSIF Consejo Nacional de Supervisión del Sistema Financiero | SUGEF Superintendencia General de Entidades Financieras | SUGEVAL Superintendencia General de Valores | SUPEN Superintendencia de Pensiones | SUGESE Superintendencia General de Seguros

Abril, 2024

Agenda

- Antecedentes.
- Estructura de la propuesta reglamentaria.
- Temas relevantes ajustados de la propuesta reglamentaria.
- Contenido de los lineamientos generales.
- Formularios para envío de observaciones.

Consulta externa

❑**Primera consulta externa:**

- ✓ El CONASSIF: Actas de las sesiones 1834-2023 y 1835-2023, celebradas el 20 de noviembre del 2023, dispuso remitir en consulta la propuesta de reglamento. Plazo 15 días hábiles. Posteriormente, dispuso extender, al 15 de enero del 2024
- ✓ SGF-3127-2023 del 29 de noviembre de 2023: Remitir en consulta la propuesta de modificación integral a los Lineamientos Generales del Reglamento. Posteriormente, se extendió al 15 de enero del 2024.

❑**Segunda consulta externa:**

- ✓ El CONASSIF: Actas de las sesiones 1853-2024 y 1854-2024, celebradas el 16 de abril del 202, dispuso remitir en consulta la propuesta de reglamento. Plazo 10 días hábiles.
- ✓ SGF-1147-2024 del 19 de abril de 2024:Remitir en consulta la propuesta de modificación integral a los Lineamientos Generales del Reglamento. Plazo 10 días hábiles.

Observaciones a la propuesta de reglamento

Distribución sectorial	Cantidad de Observaciones "Procede"	Cantidad de Observaciones "No procede"	Total
SUGEF (19)	117	247	**364**
SUGESE (5)	24	47	**71**
SUPEN (6)	23	31	**54**
SUGEVAL (Cambolsa)	0	1	**1**
Otros (3)	27	76	**103**
Total	**191**	**402**	**593**
Porcentajes	**32%**	**68%**	**100%**

Observaciones a la propuesta de lineamientos generales

	Cantidad de Observaciones "Procede"	Cantidad de Observaciones "No procede"	Total de observaciones
Cantidad	51	143	**194**
Porcentaje	26%	74%	**100%**

Temas en que se concentraron las observaciones

1. **Regulación proporcional:** Claridad y exclusiones.
2. **Definiciones:** ajustes en la redacción de algunas definiciones.
3. **Necesidad de incorporar un plazo de implementación de las disposiciones reglamentarias.**
4. **Responsabilidades de instancias de gobierno corporativo:** revisión de responsabilidades que podrían ser más de índole operativa.
5. **Disposiciones sobre bases de datos:** Revisión y ajuste, por ejemplo, temas de "accesos a bases de datos".
6. **Computación en la nube:** revisión y ajuste con base en las recomendaciones de los proveedores y observaciones de las entidades.
7. **Contratos de adhesión:** revisión y ajuste con base en las recomendaciones de los proveedores y observaciones de las entidades.
8. **Tercerización de la información, así como de bienes y servicios de TI.**
9. **Informes de comunicados de incidentes a las Superintendencias:** ajustes en plazos de remisión de informes de comunicados de incidentes.
10. **Auditoría externa de TI:** Aclaraciones sobre la periodicidad de la Auditoría

Reglamento General de Gobierno y Gestión de la Tecnología de Información

Capítulo I. Disposiciones generales

- **Artículo 1 Objeto**
- **Artículo 2 Alcance**
- **Artículo 3 Regulación proporcional**
- **Artículo 4 Definiciones y abreviaturas**
- **Artículo 5 Lineamientos Generales**

Capítulo II. Gobierno y Gestión de TI

- **Sección I: Marco de gobierno y gestión de TI (2 artículos)**
- **Sección II: Responsabilidades del Órgano de Dirección (3 artículos)**
- **Sección III: Responsabilidades de la Alta Gerencia y del Comité de TI o de la función equivalente (3 artículos)**
- **Sección IV: Responsabilidades de los Órganos de Control (2 artículos)**

Capítulo III. Organización de las tecnologías de información

- **Sección I: Generalidades de la gestión de TI (3 artículos)**
- **Sección II: Tratamiento de datos, activos de información, aplicaciones , sistemas de información y soluciones tecnológicas (3 artículos)**
- **Sección III: Gestión de la computación en la nube (3 artículos)**
- **Sección IV: Tercerización de bienes y servicios de TI (6 artículos)**

Capitulo IV. Seguridad de la información y seguridad cibernética

- **Sección I: Gestión de la seguridad de la información y de la seguridad cibernética (5 artículos)**
- **Sección II: Incidentes de seguridad de la información y seguridad cibernética (6 artículos)**

Capitulo V . Auditoría Externa de TI

- **Sección I: Perfil tecnológico (4 artículos)**
- **Sección II: Auditoría externa (6 artículos)**
- **Sección III: Reporte de supervisión y plan de acción (3 artículos)**
- **Sección VI: Prorrogas (2 artículos)**

Disposiciones adicionales (1 disposición)
Disposiciones transitorias (7 disposiciones)

Aspectos principales que se ajustaron a partir de las observaciones y comentarios

Capítulo II. Gobierno y gestión de TI / Sección I.
Artículo 7. Propósitos del marco de gobierno y gestión de TI

Acciones: se ajustó la redacción para mejorar el entendimiento de los propósitos, se modificó el orden en que estaban algunos incisos, se excluyeron aspectos que estaban repetidos.

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

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

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

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

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

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

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

Capítulo I. Disposiciones generales
Artículo 4. Definiciones

Acciones:

- **Ajustes en la redacción para mejorar el entendimiento de algunas definiciones (a partir de las observaciones):**
  - ✓ Gestión de TI.
  - ✓ Marco de gestión de TI (Ahora Marco de gobierno y gestión de TI).
  - ✓ Proveedores de bienes y servicios de TI críticos.

- **Incorporación de algunas definiciones:**
  - ✓ Activos digitales.
  - ✓ Gobierno de TI.
  - ✓ Seguridad de la información.

Capítulo II. Gobierno y gestión de TI
Secciones II y III

Acciones:

- ❑ Ajustes en la redacción de algunas responsabilidades.
- ❑ Traslado o exclusión de algunas responsabilidades que no correspondían al Órgano de Dirección.
- ❑ Modificaciones de infinitivos.

- ❑ **Las disposiciones están plenamente integradas y son complementarias al marco general de gobierno y de gestión de riesgos establecido en:**

✓ Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16.
✓ Marco de regulación vigente sobre gestión de riesgos de cada Superintendencia.

Responsabilidades sobre el gobierno de TI. **Art. 8**

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

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

Alta Gerencia

Referencia. Art. 11

Comité de TI o función equivalente

Referencia. Art. 12

Órganos de Control

Referencia. Art. 14 y 15

Auditoría interna

Función de gestión de riesgos

CONASSIF SUGEF SUGEVAL SUPEN SUGESE

Capítulo III. Organización de las tecnologías de información / Sección I
Artículo 18. Responsabilidades de la unidad de TI o de la función equivalente

- **Ajustes de redacción para mejorar el entendimiento de las disposiciones.**
- **Exclusión de responsabilidades que no correspondían a la unidad de TI.**

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

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

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

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

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

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

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

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

Capítulo III. Organización de las tecnologías de información / Sección III
Artículo 19. Clasificación de activos de información y del acceso y uso de los datos

Acciones:

- ❑ Incluir "etiquetado de activos de información".
- ❑ Excluir del artículo lo referentes a: "clasificar impacto en caso de presentarse una brecha de seguridad de la información".

"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."

Capítulo III. Organización de las tecnologías de información / Sección II
Artículo 20. Bases de datos, aplicaciones, sistemas de información y soluciones tecnológicas

Acciones:

- ❑ Ajuste de la redacción y del alcance de las disposiciones.
- ❑ Reuniones con representantes de los principales proveedores de servicios de computación en la nube.

"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."

Capítulo III. Organización de las tecnologías de información / Sección III
Artículo 22. Servicios de computación en la nube

Acciones:

- ❑ Ajuste de redacción en referencia a “modelo de responsabilidades compartidas”.
- ❑ Se eliminó lo referente a que las Superintendencias requerirán un modelo de gestión de la infraestructura tecnológica diferente al de los 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.

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

~~*a) no se cumplan los requisitos legales y de seguridad;*~~

~~*b) no se brinde acceso al supervisor, o*~~

~~*c)la información que se desea mantener en la nube sea sensible o crítica para la continuidad del negocio y no exista certeza razonada sobre la seguridad de la información y la cibernética.*~~

Capítulo III. Organización de las tecnologías de información
Sección III. Gestión de la computación en la nube

Documentación de los servicios de la computación en la nube

Acciones:

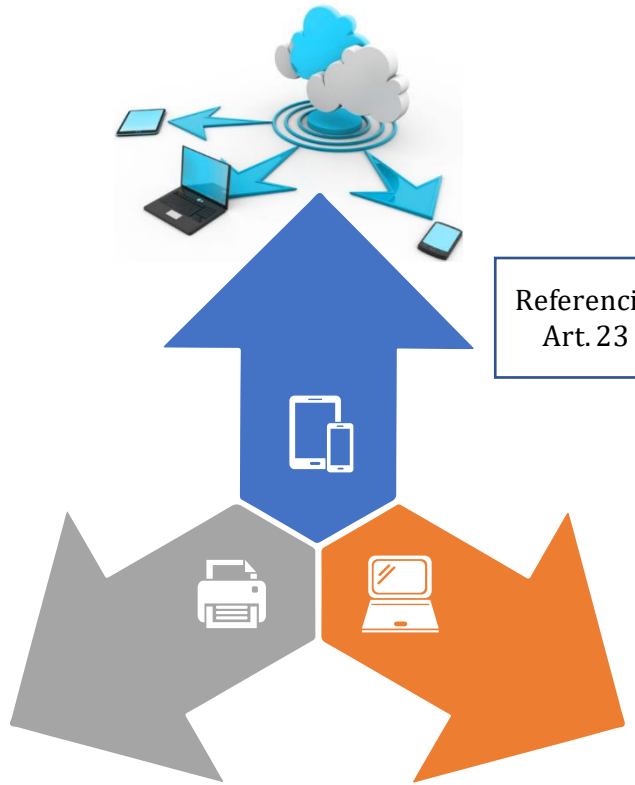
- ❑ **Ajustes dado que la documentación varía según el servicio contratado de computación en la nube.**
- ❑ **Por las características de los servicios en la nube, se optó por:**

✓ Abordaje desde la práctica supervisora.

✓ Exclusión de detalle de documentos que deba mantener la entidad.

✓ Se indica que deben "mantener la documentación de los controles administrativos y técnicos a disposición de las Superintendencias".

Referencia. Art. 24



Referencia. Art. 23

Obligaciones para uso de los servicios de la computación en la nube

Consideraciones: La clasificación de TIERs del Uptime Institute busca medir la disponibilidad y el rendimiento general de un centro de datos. Esta métrica no da la visión completa para nuevas tecnologías y modelos como la nube.

Acciones:

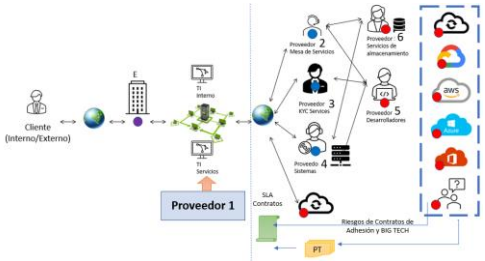
- ❑ Se ajustó la redacción y el alcance de las disposiciones.
- ❑ Se eliminó lo referente a los TIERS y al deber de disponer de informes de controles de organización de servicios : SOC2, SOC3, de las certificaciones SSAE16/SSAE18 o similares.
- ❑ Reuniones con representantes de los principales proveedores de servicios de computación en la nube.

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

Capítulo III. Organización de las tecnologías de información
Sección IV. Tercerización de bienes y servicios de TI

Acciones:

- ❑ Se ajusta la redacción.
- ❑ Se incorpora párrafo a fin de asegurar las medidas de control de seguridad de la información y seguridad cibernética cuando se delegue información confidencial o sensible a terceros.
- ❑ Reuniones con expertos de ISACA.



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

- ✓ Cuando se delegue el procesamiento, la transmisión o el almacenamiento de información clasificada como confidencial o sensible a terceros:

- ✓ Asegurar que dichos terceros implementen controles de seguridad de la información y seguridad cibernética.

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

- ✓ 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.

Capítulo III. Organización de las tecnologías de información / Sección IV
Artículo 29. Contratos y acuerdos de nivel de servicio

Acciones:

- ❑ Ajustes de redacción para mejor entendimiento de la disposición.

" […]

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.

[…]".

Artículo 30. Acceso de las Superintendencias a la información

Acciones:

- ❑ Considerar casos que tratan sobre proveedores que brindan servicios de computación en la nube.
- ❑ Reuniones con representantes de los principales proveedores de servicios de computación en la nube.
- ❑ Se ajustó la redacción y el alcance de las disposiciones.

Artículo 30. Acceso de las Superintendencias a la información

Las entidades y empresas supervisadas deben asegurar~~, a través de los contratos y los acuerdos de nivel de servicio,~~ que las Superintendencias tengan acceso a los registros, datos e información de los bienes y servicios de TI tercerizados 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
Artículo 32. Seguridad cibernética

Acciones:

- Se elimina lo referente a "establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información".

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

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

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

Acciones:

- Se elimina del alcance de los planes lo referente a "proveedores".

"[…]

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

[…]".

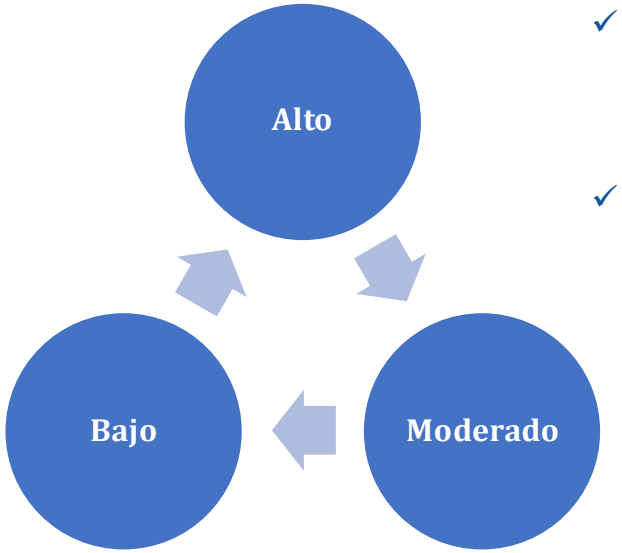
Capítulo IV. Seguridad de la información y seguridad cibernética / Sección II. Incidentes
Artículo 38. Clasificación, registro e impacto de los incidentes de seguridad de la información y seguridad cibernética

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.

Clasificación de los incidentes

- ✓ Clasificación
- ✓ Tipo de Incidente
- ✓ Descripción práctica

Clasificación de impacto



- ✓ ***Se simplificó para evitar duplicidades de clasificaciones que tratan sobre el tema impacto.***
- ✓ ***Se eliminó la clasificación para priorizar el impacto (Funcional, información, capacidad de recuperación).***
- ✓ ***Se generaba confusión para las entidades.***

CONASSIF SUGEF SUGEVAL SUPEN SUGESE

Capítulo IV. Seguridad de la información y seguridad cibernética / Sección II. Incidentes
Artículo 39. Comunicación de incidentes de seguridad de la información y seguridad cibernética a las Superintendencias

❑ **Comunicado inicial a las respectivas Superintendencias:**

- ✓ Incidentes de seguridad de la información y seguridad cibernética cuando su impacto sea clasificado como "moderado" o "alto".
- ✓ A más tardar ocho horas contadas a partir de identificado el incidente y de establecido su impacto o afectación.

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

1. Informe de atención de incidentes:

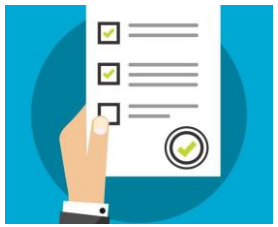
- ✓ Informe oficial de la entidad o empresa supervisada donde se detalla el incidente de seguridad de la información o de seguridad cibernética revelado en el comunicado.

2. Informe de seguimiento de atención de incidentes:

- ✓ Informe de seguimiento de actividades para atender el incidente de seguridad de la información o seguridad cibernética.

3. Informe post- actividades de incidentes:

- ✓ Incluye, al menos, reporte de costes, los reportes técnicos y de análisis forense, así como lecciones aprendidas.



Capítulo IV. Seguridad de la información y seguridad cibernética / Sección II. Incidentes
Artículo 40. Comunicado de incidentes a los clientes

- 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.

- Definir el tipo, el alcance y el contenido mínimo de la comunicación.

- 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.

Capítulo IV. Seguridad de la información y seguridad cibernética / Sección II. Incidentes
Artículo 41.Reporte histórico de incidentes de seguridad de la información y seguridad cibernética

Acciones:

- ❑ Se modifica la redacción del artículo.
- ❑ se elimina lo referente a que las entidades deban remitir el reporte histórico de incidentes.

"Las entidades y empresas supervisadas deben elaborar un reporte histórico de los incidentes de seguridad de la información y seguridad cibernética. Dicho reporte deberá estar a disposición de las Superintendencias cuando estas lo requieran como parte de las labores de supervisión.

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

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

Capítulo V. La auditoría externa de TI / Sección II
Artículo 46. Auditoría externa de TI

Acciones:

Se incluye párrafo para contemplar casos de proveedores de servicios de computación en la nube que ya tienen evaluaciones y auditorías, las cuales, hacen públicas y cumplen con las sanas prácticas.

[...]

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

La auditoría externa de TI deberá ser realizada de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA, salvo en los casos en que se trate de proveedores de servicios de computación en la nube que ya cuentan con auditorías independientes.

[...]

Capítulo V. La auditoría externa de TI / Sección II
Artículo 48.Periodicidad de las auditorías externas de TI

Acciones:

❑ Modificar la periodicidad para que sea cada tres años.

- ✓ Periodicidad de auditorías externas:
  Cada ~~2~~ 3 años.
- ✓ Excepto cuando el supervisor considere la necesidad de anticiparla o aplazarla.

Capítulo V. La auditoría externa de TI / Sección IV
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.*

[…]

Disposición transitoria sexta. Perfil tecnológico

"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.

Mientras tanto, 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 en los sitios electrónicos oficiales de cada Superintendencia."

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. Informes de comunicados de incidentes de seguridad cibernética a las Superintendencias
Artículo 40. Comunicado de incidentes a los clientes
Artículo 41. Reporte histórico de incidentes
Artículo 42. Perfil tecnológico
Artículo 45. Comunicación de cambios significativos del perfil tecnológico
Artículo 47. Alcance y plazo de la auditoría externa de TI
Artículo 48. Periodicidad de las auditorías externas de TI

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

Lineamientos Generales

Condiciones para tipificar la gestión de TI, el Comité de TI o sus funciones equivalentes como corporativos.

Modelo de clasificación de activos de información.

Elementos que las entidades y empresas supervisadas incorporarán en el diseño de los contratos y de 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.

Clasificación para el registro de incidentes de seguridad de la información y seguridad cibernética, sus tipos de incidentes.

Tipos, plazos y formatos de los informes de incidentes de seguridad de la información y seguridad cibernética.

Elementos necesarios que guiarán a las entidades y empresas supervisadas en la aplicación de las disposiciones establecidas sobre auditorías externas de TI.

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 para el plazo de la remisión del plan de acción.

Anexos.

Formularios para envío de observaciones
Segunda consulta externa

Estimada señora:

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

considerando que:

A. El numeral 2 del artículo 361 de la *Ley General de la Administración Pública*, Ley 6227, establece que se concederá a las entidades representativas de intereses de carácter general o corporativo afectadas por la disposición, la oportunidad de exponer su parecer.

B. Se elaboró el *Reglamento General de Gobierno y Gestión de la Tecnología de Información*, en cumplimiento del *Procedimiento para la Tramitación ante el Consejo Nacional de Supervisión del Sistema Financiero Costarricense de proyectos de emisión o reforma de reglamentos del sistema financiero*, el cual debe ser sometido en consulta a las entidades supervisadas, cámaras y gremios, así como a los grupos y conglomerados financieros.

dispuso en firme:

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

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

SUGEF Superintendencia General de Entidades Financieras
SUGEVAL Superintendencia General de Valores
SUPEN Superintendencia de Pensiones
SUGESE Superintendencia General de Seguros

Circular Externa
19 de abril de 2024
SGF-1147-2024
C03/0-683
SP-409-2024
SGS-C-0050-2024
SGF-PUBLICO

- ✓ **Herramienta: *Microsoft Forms***
- ✓ **Un formulario para la propuesta reglamentaria y otro formulario para los lineamientos generales**

CONASSIF Consejo Nacional de Supervisión del Sistema Financiero
SUGEF Superintendencia General de Entidades Financieras
SUGEVAL Superintendencia General de Valores
SUPEN Superintendencia de Pensiones
SUGESE Superintendencia General de Seguros

Formularios para envío de observaciones
Segunda consulta externa

Formularios para remitir observaciones de normativa en consulta

Reglamentos	Fecha de Inicio	Fecha Final	Referencia
Modificación al *Reglamento General de Gestión de la Tecnología de Información*, Acuerdo Conassif 5-17	18/04/2024	2/05/2024	CNS-1853-2024 CNS-1854-2024. Art 6 y 5 17/04/2024
Modificación integral a los Lineamientos Generales del Reglamento General de Gestión de la Tecnología de Información, Acuerdo Conassif 5-17	23/04/2024	7/05/2024	SGF-1147-2024 19/04/2024

¡Muchas Gracias!

CONASSIF Consejo Nacional de Supervisión del Sistema Financiero
SUGEF Superintendencia General de Entidades Financieras
SUGEVAL Superintendencia General de Valores
SUPEN Superintendencia de Pensiones
SUGESE Superintendencia General de Seguros