CONASSIF SUGEF SUGESE SUGEVAL SUPEN

Consulta

- “Modificación integral del Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17”
- Lineamientos Generales

Diciembre, 2023

Agenda

- Antecedentes.
- Estructura de la propuesta reglamentaria.
- Temas medulares de la propuesta reglamentaria.
- Gestión de la seguridad de la información y seguridad cibernética.
- Formularios para envío de observaciones.

Antecedentes

AUMENTO EN LA DIGITALIZACIÓN, PLATAFORMAS BASADAS EN INTERNET.

USO CRECIENTE DE TERCEROS PROVEEDORES DE SERVICIOS.

AUMENTO EN LOS CIBERATAQUES.

PROTECCIÓN DE LA INFORMACIÓN .

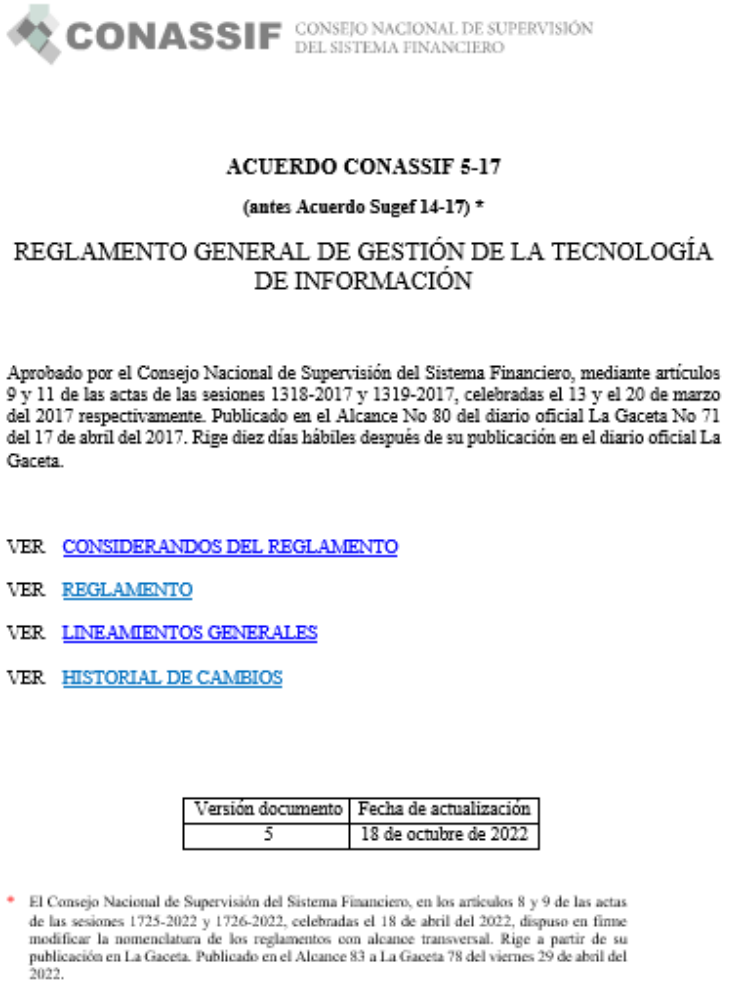
CONSIDERACIONES SOBRE LA ESTABILIDAD Y CONFIANZA EN EL SISTEMA.

ACTUALMENTE EL ABORDAJE DE LA SEGURIDAD CIBERNÉTICA NO ES EXCLUSIVO DE LAS ÁREAS DE TI.

Proyecto transversal: Marco General de Gobierno y Gestión de la Tecnología y la Información

Objetivo general del proyecto:

Proponer un marco de regulación y fortalecer los procesos de supervisión del riesgo de ciberseguridad, incluyendo la actualización del estándar de referencia y el reforzamiento del marco de gestión de TI, con el fin de minimizar el impacto de las posibles amenazas e incidentes que comprometan la estabilidad del Sistema Financiero Nacional.



CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

ACUERDO CONASSIF 5-17

(antes Acuerdo Sugef 14-17) *

REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, 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. Publicado en el Alcance No 80 del diario oficial La Gaceta No 71 del 17 de abril del 2017. Rige diez días hábiles después de su publicación en el diario oficial La Gaceta.

VER CONSIDERANDOS DEL REGLAMENTO

VER REGLAMENTO

VER LINEAMIENTOS GENERALES

VER HISTORIAL DE CAMBIOS

Versión documento	Fecha de actualización
5	18 de octubre de 2022

* El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 9 de las actas de las sesiones 1725-2022 y 1726-2022, celebradas el 18 de abril del 2022, dispuso en firme modificar la nomenclatura de los reglamentos con alcance transversal. Rige a partir de su publicación en La Gaceta. Publicado en el Alcance 83 a La Gaceta 78 del viernes 29 de abril del 2022.

Justificación

- **Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17:** establece los requerimientos mínimos para la gestión de la tecnología de información

- Los estándares relacionados con TI han evolucionado para incorporar nuevos alcances en relación con:

✓ Servicios de computación en la nube

✓ tercerización de bienes y servicios de TI

✓ El tratamiento del uso y acceso de los datos y de los activos de información

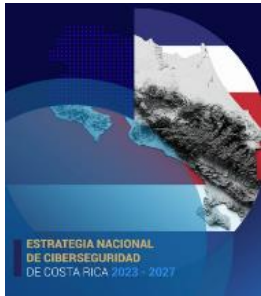
✓ Tecnologías emergentes.

Estrategia Nacional de Ciberseguridad-Costa Rica

Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica

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.

Papel del regulador: incluye contar con un marco normativo basado en buenas prácticas para la protección de infraestructuras críticas



Diagnóstico de la situación actual y brechas en ciberresiliencia

Diagnóstico de la situación actual y brechas en ciberresiliencia del marco vigente establecido en el Acuerdo CONASSIF 5-17 para determinar si la regulación y la supervisión contribuyen en promover un sistema financiero ciberresiliente.

Para el análisis de brechas se abarcaron diferentes temas:

- ✓ Evolución de la regulación para el sector financiero.
- ✓ Regulación de la gestión de TI.
- ✓ Seguridad cibernética en la regulación actual.
- ✓ Estándares, marcos y mejores prácticas de aceptación internacional utilizados para la supervisión y regulación en materia de seguridad cibernética. COBIT NIST ISO

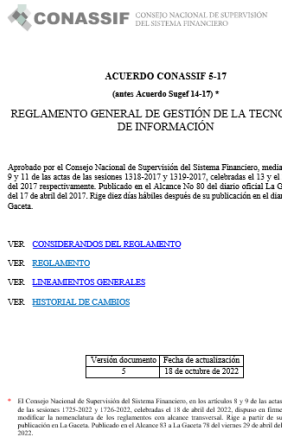
Cuestionario sobre ciberseguridad Mayo-Julio 2022

Asistencias técnicas:
CAPTAC-DR
Toronto Centre

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

Modificación integral con el fin de alcanzar los siguientes propósitos:

1. **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.**
   - ✓ Seguridad de la información.
   - ✓ Seguridad cibernética.
   - ✓ Resiliencia operativa digital.
2. **Actualizar el marco de gobierno y de gestión de TI e incorporar disposiciones.**
   - ✓ Tecnologías emergentes.
   - ✓ Gobierno y gestión de la seguridad de la información, seguridad cibernética, incidentes de seguridad cibernética.
   - ✓ Tercerización de bienes y servicios de TI.
   - ✓ Computación en la nube.
   - ✓ Tratamiento del uso y acceso de los datos y de los activos de información.



CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

ACUERDO CONASSIF 5-17

(antes Acuerdo Sugef 14-17) *

REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, 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. Publicado en el Alcance No 80 del diario oficial La Gaceta No 71 del 17 de abril del 2017. Rige diez días hábiles después de su publicación en el diario oficial La Gaceta.

VER. CONSIDERANDOS DEL REGLAMENTO

VER. REGLAMENTO

VER. LINEAMIENTOS GENERALES

VER. HISTORIAL DE CAMBIOS

Versión documento	Fecha de actualización
5	18 de octubre de 2022

* El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 8 y 9 de las actas de las sesiones 1725-2022 y 1726-2022, celebradas el 18 de abril del 2022, dispuso en firme modificar la nomenclatura de los reglamentos con alcance transversal. Rige a partir de su publicación en La Gaceta. Publicado en el Alcance 83 a La Gaceta 78 del viernes 29 de abril del 2022.

Reglamento General de Gobierno y Gestión de la Tecnología de Información

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

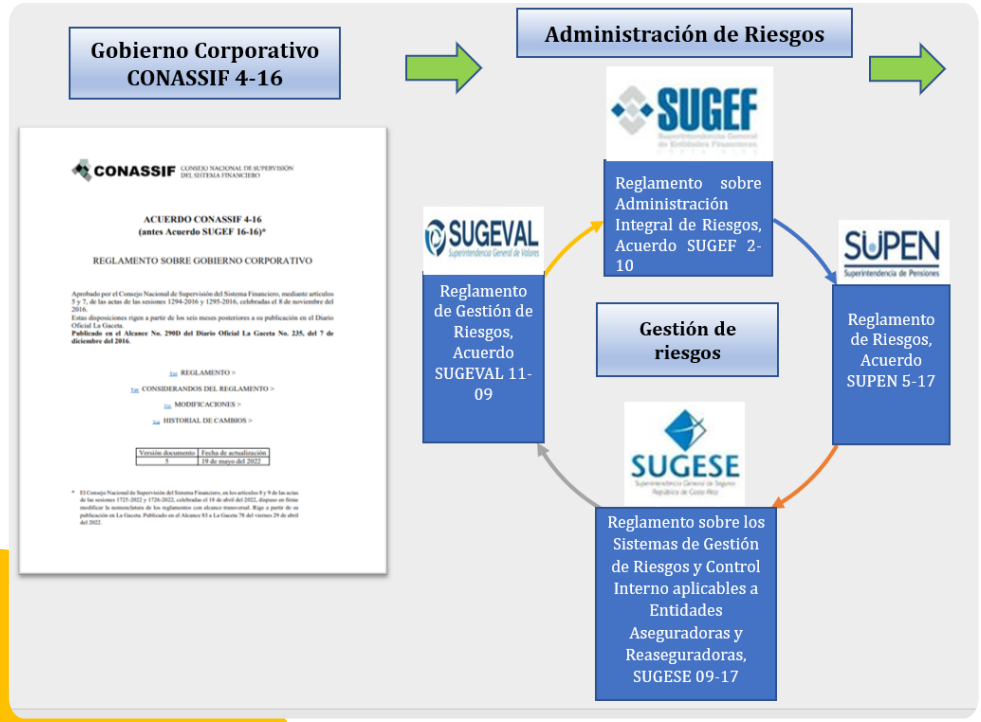
- Sección I: Gestión de la seguridad de la información y de la seguridad cibernética (5 artículos)
- Sección II: Incidentes de seguridad cibernética (6 artículos)

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 (5 disposiciones)

Capítulo I. Disposiciones generales



Artículo 1. Objeto

1. Requerimientos para el gobierno y la gestión de la tecnología de información y sus riesgos asociados.

2. Regulación plenamente integrada y complementaria al marco general de gobernanza y de gestión de riesgos establecido en:

✓ Reglamento de Gobierno Corporativo, Acuerdo CONASSIF 4-16 y en el

✓ Marco de regulación vigente sobre gestión de riesgos de cada superintendencia.

Capítulo I. Disposiciones generales

Artículo 2. Alcance.

Las disposiciones establecidas en el 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, y
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.

e) Controladoras y empresas integrantes de grupos y conglomerados financieros supervisados, en los casos en que así lo requiere el supervisor responsable.

Capítulo I. Disposiciones generales
Proporcionalidad en la Regulación de TI

Los siguientes alcances del Reglamento se consideran como referencias sobre sanas prácticas que discrecionalmente podrán adoptar las entidades:

1. Responsabilidades del Órgano de Dirección sobre el gobierno de TI, la seguridad cibernética y la resiliencia operativa digital.
2. Responsabilidades de la Alta Gerencia, del Comité de TI o de la función equivalente y de los Órganos de Control sobre la gestión de TI.
3. Establecimiento de una Unidad de TI y sus responsabilidades.
4. Tratamiento de datos, activos de información, aplicaciones, sistemas de información y soluciones tecnológicas.
5. Gestión de la computación en la nube.
6. Tercerización de bienes y servicios de TI.

- ✓ Regulación proporcional para cooperativas de ahorro y crédito, Acuerdo SUGEF 25-23
- ✓ Sociedades Corredoras de Seguros

Referencia. Art. 3

Capítulo I. Disposiciones generales
Proporcionalidad en la Regulación de TI

Los siguientes alcances sobre seguridad de la información y seguridad cibernética, serán de aplicación plena:

1. Diseñar, implementar, mantener y monitorear un sistema de gestión de la seguridad de la información.
2. Gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital.
3. Gestión y comunicado de incidentes de seguridad cibernética.

Referencia.
Art. 3

Capítulo I. Disposiciones generales
Proporcionalidad en la Regulación de TI

También serán aplicables disposiciones sobre la auditoría externa:

1. Perfil tecnológico
2. Comunicación de cambios significativos del perfil tecnológico.
3. Alcance y periodicidad de la Auditoría Externa de TI.
4. Productos de la auditoría externa de TI.
5. Plan de acción para la gestión de los hallazgos y los riesgos identificados como resultado de la auditoría externa de TI.

Referencia.
Art. 3

Capítulo I. Disposiciones generales
Proporcionalidad en la Regulación de TI

Referencia.
Art. 3

a) Periodicidad de auditorías externas:

- ✓ Cada tres años.
- ✓ Excepto cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de anticiparla o aplazarla.

b) Alcance de las auditorías externas Cooperativas (13 procesos)

1. Gestionar el marco de gestión de TI.
2. Gestionar la estrategia.
3. Gestionar el presupuesto y los costos.
4. Gestionar los acuerdos de servicio.
5. Gestionar los proveedores.
6. Gestionar el riesgo.
7. Gestionar la seguridad.
8. Gestionar los cambios.
9. Gestionar los activos.
10. Gestionar peticiones e incidentes de servicio.
11. Gestionar la continuidad.
12. Gestionar servicios de seguridad.
13. Supervisar, evaluar y valorar el sistema de control interno.

Capítulo I. Disposiciones generales
Proporcionalidad en la Regulación de TI

c) Alcance de las auditorías externas sociedades corredoras de seguros (9 procesos)

1. Gestionar el marco de gestión de TI
2. Gestionar los acuerdos de servicio
3. Gestionar los proveedores
4. Gestionar el riesgo
5. Gestionar la seguridad
6. Gestionar peticiones e incidentes de servicio
7. Gestionar la continuidad
8. Gestionar servicios de seguridad
9. Supervisar, evaluar y valorar el sistema de control interno

Referencia.
Art. 3

Capítulo II. Gobierno y gestión de TI

Artículo 6. Desarrollo del Marco de gobierno y gestión de TI

- Diseñar, implementar, controlar y mantener un marco de gobierno y gestión de TI de conformidad con:

✓ Estrategia organizacional.
✓ Apetito de riesgo
✓ Nivel de tolerancia al riesgo
✓ Políticas aprobadas por el Órgano de Dirección.

- 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.

Capítulo II. Gobierno y gestión de TI
Sección II. Responsabilidades del Órgano de Dirección.

Responsabilidades sobre el gobierno de TI. — Art. 8

- ✓ Aprobar marco de gobierno y gestión de TI.
- ✓ Establecer Comité de TI.
- ✓ Aprobar las políticas, estructuras, planes estratégicos, recursos, inversiones y presupuestos.

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

- ✓ Gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética, integrados dentro de la gestión de riesgos.
- ✓ Asignar tiempo a las discusiones sobre la gestión de los riesgos de seguridad de la información y de seguridad cibernética.
- ✓ Establecimiento de un sistema de gestión de la seguridad de la información.

Responsabilidades sobre la resiliencia operativa digital. — Art. 10

- ✓ Asegurar la resiliencia operativa digital para la continuidad de las operaciones.
- ✓ Estrategia de la resiliencia operativa digital.
- ✓ Implementación de planes de respuesta, recuperación y atención de crisis para gestionar los incidentes de seguridad cibernética .

Capítulo II. Gobierno y gestión de TI

Sección III. Responsabilidades de la Alta Gerencia y del Comité de TI.
Sección IV. Responsabilidades de los Órganos de Control

Referencia. Art. 11

Alta Gerencia

1. Implementar el marco de gobierno y gestión de TI.
2. Proponer al Órgano de Dirección las estrategias y los recursos.
3. Implementar los planes de acción para la atención de los hallazgos de la auditoría externa de TI.

Referencia. Art. 12

Comité de TI

1. Supervisar la implementación del marco de gobierno y gestión de TI.
2. Asesorar al Órgano de Dirección y a la Alta Gerencia en la formulación de las estrategias y las metas de TI.

Órganos de control

Auditoría interna

1. Supervisar el cumplimiento de las políticas y los procedimientos que se establezcan en relación con TI.
2. Evaluar la calidad y eficacia de los planes de acción que atenderán los hallazgos de la auditoría externa de TI.

Gestión de riegos

1. Incorporar la gestión de los riesgos tecnológicos, de la seguridad de la información y de la seguridad cibernética dentro de la gestión de riesgos de la entidad o empresa supervisada.

Referencia Art. 14,15

Capítulo III. Organización de las tecnologías de información

Gestión de TI

Referencia.
Art. 16

Tipificada de manera predeterminada como gestión de TI individual

✓ **Gestión de TI corporativa**

01

Grupos y Conglomerados financieros

Supervisor responsable

Un permiso para tipificar su gestión de TI como corporativa

02

- ✓ Coordinar, aplicar y mantener un único marco de gobierno y de gestión de TI.
- ✓ 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.

03

- ✓ Solicitud: Justificación debidamente sustentada que demuestre que se cumplen las condiciones para que la gestión de TI sea tipificada como corporativa.
- ✓ Lineamientos generales.

04

- ✓ No atiende en forma adecuada y oportuna las funciones y obligaciones indicadas en el 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.

Capítulo III. Organización de las tecnologías de información

Unidad de TI o función equivalente

Establecer una Unidad de TI o una función equivalente encargada de:

Referencia. Art. 17

- Implementar y desarrollar soluciones tecnológicas para apoyar y facilitar la ej
procesos interno.

-Marco de gobierno y gestión de TI.

Referencia. Art. 18

Responsabilidades

a) Ejecutar las acciones del marco de gobierno y gestión de TI que le correspondan a la entidad o empresa supervisada.

b) Gestionar los riesgos tecnológicos de conformidad con el apetito y la tolerancia del riesgo de la entidad o empresa supervisada.

c) Desarrollar la planificación y la estrategia de TI, las cuales deben estar alineadas con los objetivos estratégicos establecidos por la entidad o empresa supervisada.

Tratamiento de datos, activos de información, aplicaciones, sistemas de información y soluciones tecnológicas

- ✓ Clasificar activos de información, el impacto potencial en caso de presentarse una brecha de seguridad de la información, el acceso y uso de los datos y los activos de información.

- ✓ **Bases de datos actualizadas, las aplicaciones, los sistemas de información y las soluciones tecnológicas vigentes que procesan o dan acceso a las bases de datos de las entidades o empresas supervisadas:** estar disponibles y accesibles a las Superintendencias.

- ✓ 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.

Referencia.
Art. 19,20,21

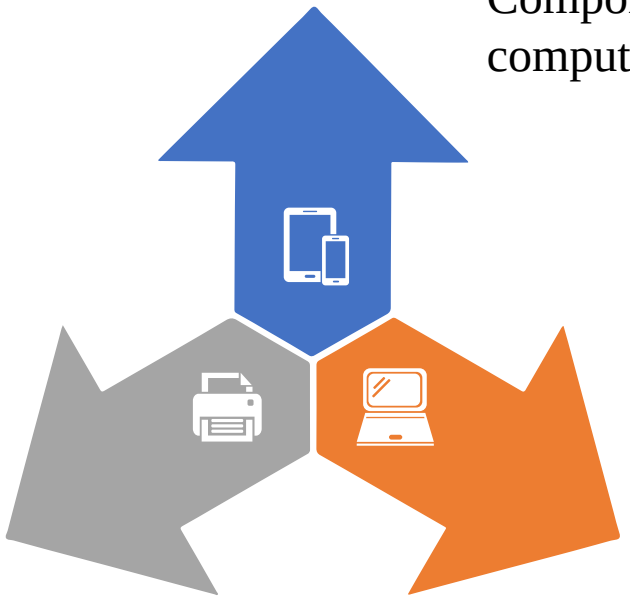
Capítulo III. Organización de las tecnologías de información

Gestión de la computación en la nube

A-Servicios de computación en la nube

Componentes tecnológicos mediante servicios de computación en la nube.

Referencia. Art. 22



B-Obligaciones generales para el uso de la computación en la nube

1. Gestión efectiva de los riesgos.
2. Criterios para seleccionar el proveedor.
3. Respaldo de la información que se procesa en la nube.

Referencia. Art. 23

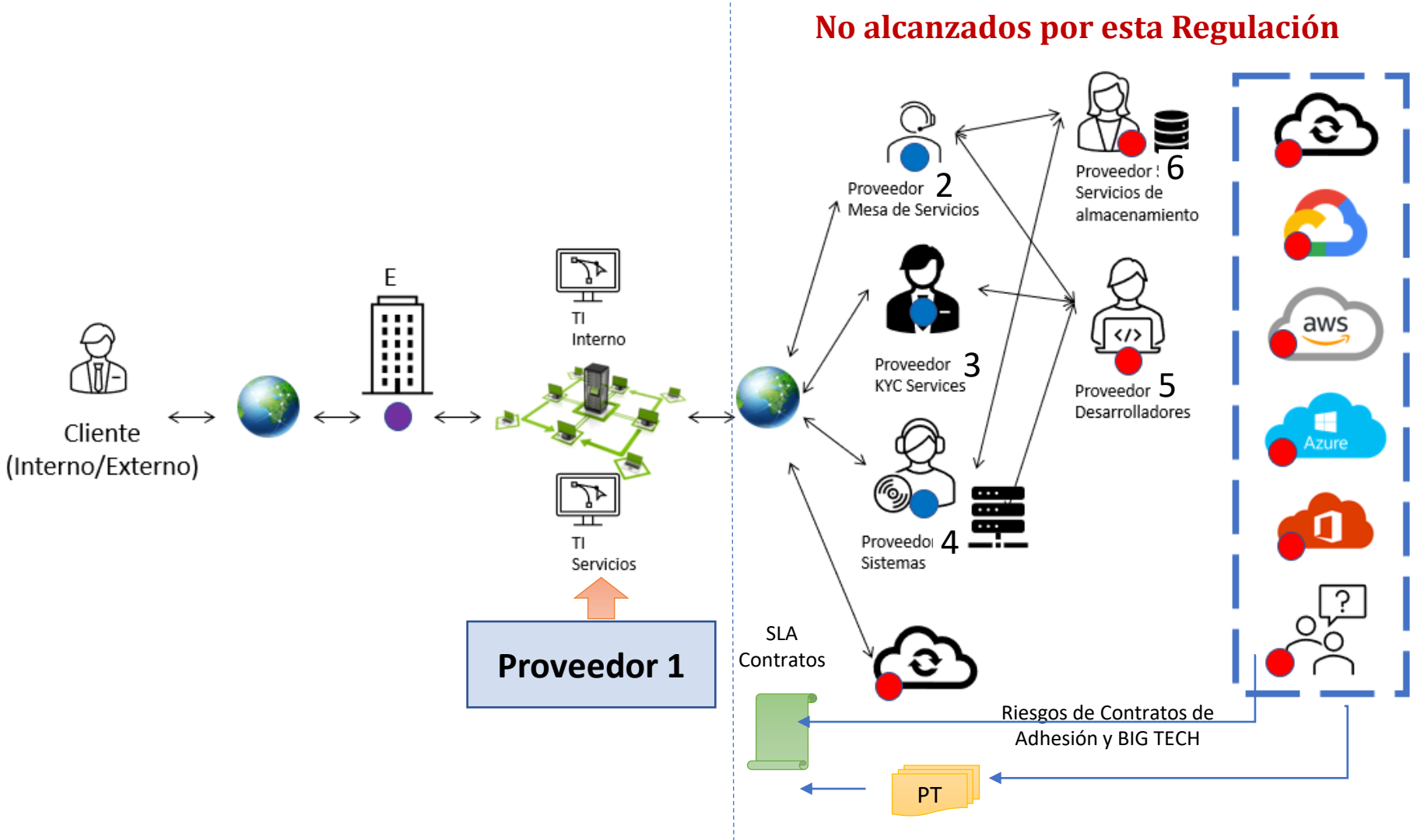
C-Documentación de los servicios de la computación en la nube

Mantener actualizada y a disposición permanente de las Superintendencias la documentación de los servicios de la computación en la nube.

Referencia. Art. 24

Capítulo III. Organización de las tecnologías de información

Tercerización de bienes y servicios de TI



Capítulo III. Organización de las tecnologías de información

Tercerización de bienes y servicios de TI

Son responsabilidades de la entidad o empresa supervisada:

Referencia.
Art. 25 al 30

- ✓ Gobierno, la gestión.
- ✓ Seguridad de la información.
- ✓ Seguridad cibernética.
- ✓ Bienes y servicios tecnológicos.
- ✓ Resiliencia operativa digital.

✓ Identificación de riesgos de bienes y servicios de TI proveídos por terceros

✓ Acceso de las Superintendencias a la información.

Continuidad del servicio mediante cláusulas contractuales y acuerdos de nivel de servicio

Capítulo IV. Gestión de la seguridad de la información y de la seguridad cibernética

CAPÍTULO IV SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD CIBERNÉTICA

Sección I. Gestión de la seguridad de la información y de la seguridad cibernética
Artículo 31. Sistema de gestión de la seguridad de la información.
Artículo 32. Seguridad cibernética.
Artículo 33. Programas de análisis de vulnerabilidades y pruebas.
Artículo 34. Unidades, funciones organizacionales, centros de operaciones y comités técnicos de gestión riesgos de seguridad cibernética.
Artículo 35. Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética.

Sección II. Incidentes de seguridad cibernética
Artículo 36. Gestión de incidentes de seguridad cibernética.
Artículo 37. Función de respuesta a incidentes de seguridad cibernética.
Artículo 38. Clasificación, registro y priorización de los incidentes de seguridad cibernética.
Artículo 39. Informes de comunicados de incidentes de seguridad cibernética a las Superintendencias.
Artículo 40. Comunicado de incidentes a las partes interesadas.
Artículo 41. Reporte histórico de incidentes.

Sistema de gestión de la seguridad de la información

Diseño, implementación, mantenimiento y monitoreo de un sistema de gestión de la seguridad de la información que incluya las disposiciones de seguridad cibernética del reglamento.

Referencia.
Art. 31

Implementación: 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.

Seguridad cibernética

1. Gestionar la seguridad cibernética para cumplir con los requerimientos del negocio y asegurar una resiliencia operativa digital.

2. Establecer si la seguridad cibernética está integrada o separada del sistema de gestión de la seguridad de la información.

3. Establecer indicadores para medir de forma recurrente la eficacia y eficiencia de la seguridad cibernética.

Referencia.
Art. 32

Programas de análisis de vulnerabilidades y pruebas

- ✓ Establecer programas de análisis de vulnerabilidades y pruebas que incluyan los controles de seguridad de la información y seguridad cibernética.

- ✓ **Análisis de vulnerabilidades, así como los tipos de pruebas y sus alcances:** acordes con los riesgos de seguridad de la información y seguridad cibernética.

Referencia.
Art. 33

Unidades, funciones organizacionales, centros operacionales o comités técnicos de gestión de riesgos de seguridad cibernética

Establecimiento de las unidades, funciones organizacionales, centros de operaciones o comités relacionados con la seguridad cibernética

- ✓ Pueden estar integradas a las áreas o funciones de seguridad de la información de la organización, externalizadas o de forma separada a la gestión de la seguridad de la información.

- ✓ Estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por la organización.

Referencia.
Art. 34

Planes de promoción de la cultura de la seguridad de la información y de la seguridad cibernética

- Diseñar e implementar planes de promoción de la cultura sobre la seguridad de la información y la seguridad cibernética.

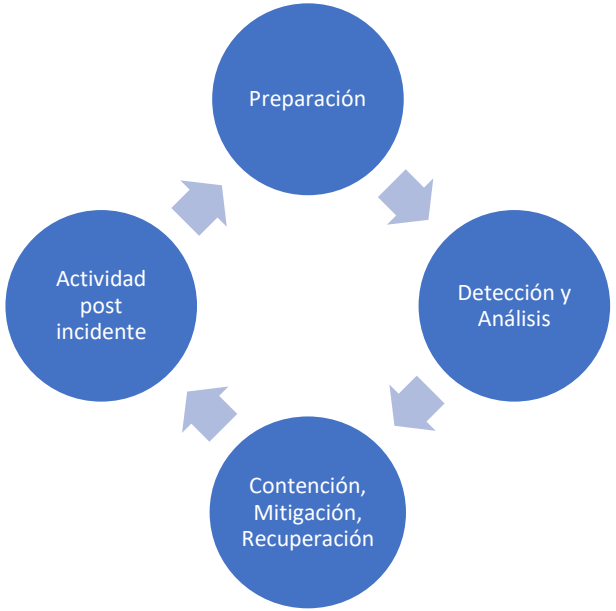
- Actividades de capacitación, concientización, divulgación, comunicación y promoción de una cultura organizacional de seguridad de la información y de seguridad cibernética dirigidos a:

  ✓ Colaboradores, clientes, proveedores y demás partes interesadas.

Referencia.
Art. 35

Gestión de incidentes de seguridad cibernética

Fases de la gestión de incidentes



1. Diseño e implementación de un proceso para la gestión de incidentes de seguridad cibernética.

2. El proceso de gestión de incidentes debe establecer:

- ✓ Un plan de respuesta a incidentes de seguridad cibernética.
- ✓ Los controles para recopilar las evidencias para análisis forenses durante el seguimiento del incidente.

Referencia.
Art. 36

Función de respuesta a incidentes de seguridad cibernética

- Función de respuesta a incidentes de seguridad cibernética, de conformidad con:

  ✓ Estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados.

- Conformada por personal de diferentes áreas de la entidad o empresa supervisada, o cualquier otro miembro que se considere necesario.

Referencia.
Art. 37

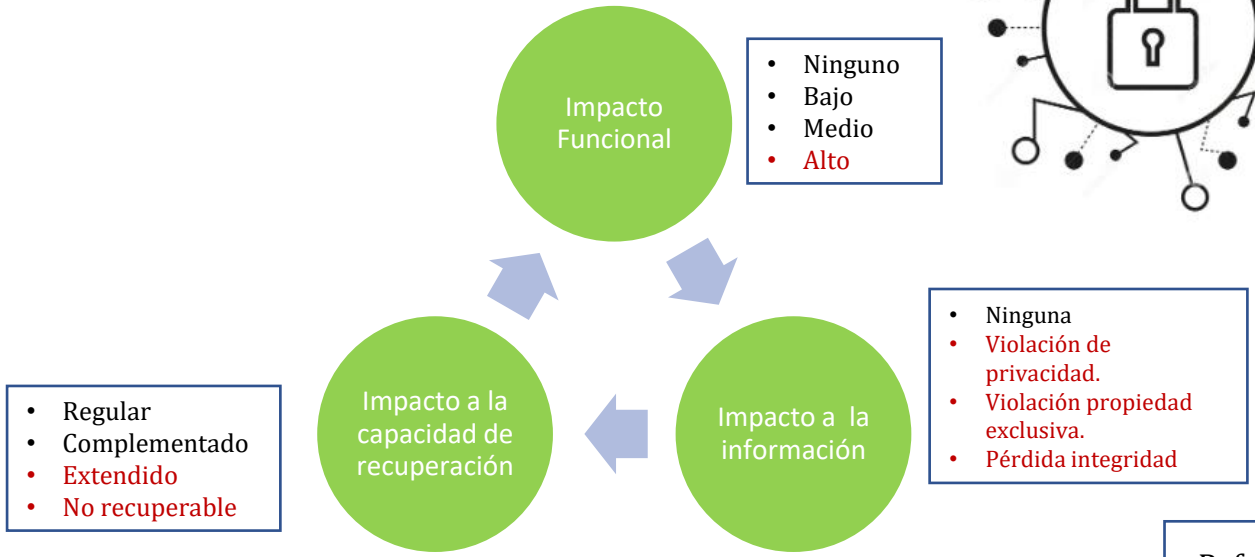
Clasificación, registro y priorización de los incidentes de seguridad cibernética

Clasificar, registrar y priorizar los incidentes de seguridad cibernética de conformidad con el esquema de clasificación y las categorías de impacto que están establecidos en los lineamientos generales del reglamento.

Esquema de clasificación de incidentes

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

Categorías de impacto



Referencia. Art. 38

Informes de comunicados de incidentes de seguridad cibernética a las Superintendencias

1. Informe inicial:

a) Informe oficial de la entidad o empresa supervisada donde se comunica el incidente de seguridad cibernética cuando:

1. Presente un impacto funcional en la organización "alto";

2. Presenten un impacto a la información en "violación de la privacidad, violación de la propiedad exclusiva o pérdida de integridad", o

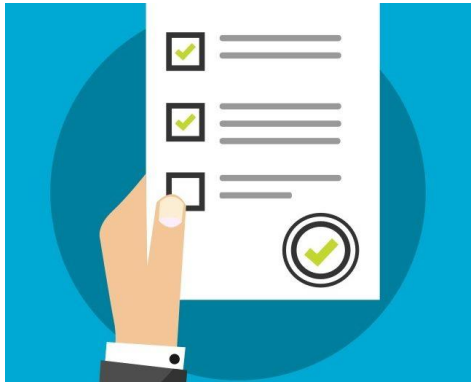
3. El impacto a la capacidad de recuperación sea "extendido" o "no recuperable".

b) El informe inicial será remitido a la respectiva Superintendencia sin demora, y a más tardar ocho horas después de identificado el incidente, de identificado el impacto a la organización o de identificada la afectación. En este informe se indicarán los miembros que conforman la función de respuesta a incidentes de seguridad cibernética.

2. Informe de avance de atención de incidentes:

a) Informe de seguimiento de actividades para atender el incidente de seguridad cibernética que fue comunicado mediante el "informe inicial".

b) El informe de avance será remitido a más tardar una semana después del comunicado del informe inicial, y, en caso de ser necesario, los siguientes informes de avance serán remitidos según el cronograma establecido en el informe inicial.



3. Informe post- actividades del incidente:

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

b) El informe post-actividades será remitido a la respectiva Superintendencia una vez cerrado el incidente de seguridad cibernética y a más tardar diez días hábiles después de cerrado el incidente.

Referencia.
Art. 39

Comunicado de incidentes a los clientes

- ✓ Confidencialidad o integridad de la información de los clientes afectada debido a un incidente de seguridad cibernética: comunicar a estos sobre la afectación.
- ✓ 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 dos días hábiles posteriores al cierre del incidente.

Referencia.
Art. 40

Reporte histórico de incidentes

Reporte histórico de los incidentes de seguridad cibernética cerrados que tuvieron un impacto funcional de sus sistemas de TI “medio” y “alto”, los cuales presenten un impacto de “pérdida de integridad” de la información o que el impacto a la capacidad de recuperación sea “complementado”, “extendido” o “no recuperable”.

Referencia.
Art.41

Entidades y empresas supervisadas por	Canales		Frecuencia (Ver nota 1)
	Mecanismo de envío	Medio (Clase de datos)	
SUGEF	SICVECA	XML de reporte de incidentes de seguridad cibernética.	Cortes a marzo, julio y noviembre.
SUGEVAL	SICVECA	XML de reporte de incidentes de seguridad cibernética.	Cortes a marzo, julio y noviembre.
SUPEN	Plataforma VES	Ventana Electrónica de Servicios	Cortes a marzo, julio y noviembre.
SUGESE	Hecho relevante	Formulario Reporte de incidentes. Publicado en sitio web de SUGESE; Solicitud de requerimiento a través de SUGESE en Línea.	Contra solicitud de requerimiento por parte de la Superintendencia .

Nota 1: *el corte al 31 de marzo cubre los meses de: diciembre, enero, febrero y marzo. El corte al 31 de julio cubre los meses de: abril, mayo, junio y julio. El corte al 30 de noviembre cubre los meses de: agosto, setiembre, octubre y noviembre.*

a. *Plazo: el reporte histórico de incidentes será remitido a más tardar diez días hábiles posteriores al cierre de los meses de marzo, julio y noviembre.*

Transitorio

a. *En el caso de las entidades y empresas supervisadas por SUGEF y SUGEVAL, el primer reporte de incidentes se remitirá con fecha de corte a julio de 2025 y cubrirá el periodo indicado en la Nota 1.*

b. *En lo sucesivo, se aplica la periodicidad establecida en los lineamientos.*

Perfil tecnológico

- ✓ Actualizarlo anualmente.

- ✓ **Gestión de TI corporativa, un Comité de TI corporativo o sus respectivas funciones equivalentes a nivel corporativo:** el grupo o conglomerado financiero podrá remitir un único perfil tecnológico al supervisor responsable.

- ✓ El 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.

Referencia.
Art.42

Capítulo V. Auditoría Externa de TI

Procesos de evaluación del marco de gobierno y de gestión de TI

Referencia.
Art. 42,43

Indicar en el perfil tecnológico cuáles de los procesos de evaluación detallados en los lineamientos generales del reglamento resultan adecuados a su marco de gobierno y gestión de TI

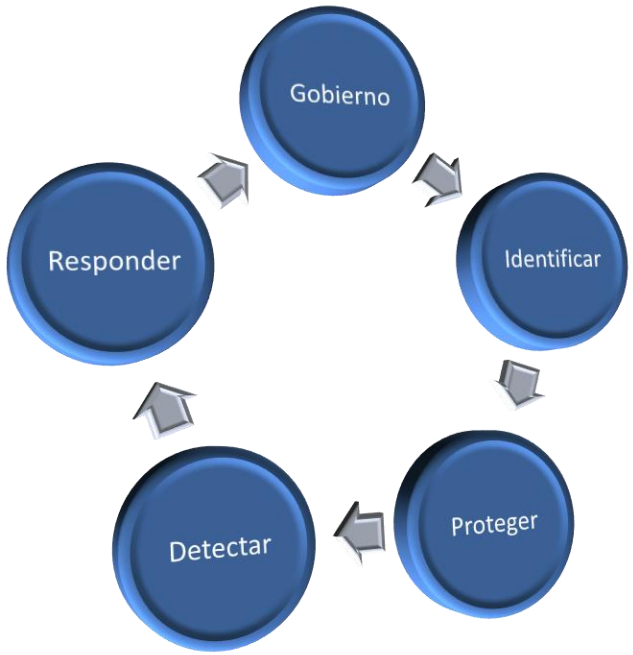
Los procesos que no aplican para su modelo de negocio deberán ser justificados mediante un estudio técnico

Las Superintendencias pueden requerir la inclusión de procesos de evaluación en el perfil tecnológico

Motivos: necesidades de supervisión, el riesgo identificado, o cuando se determine que los marcos de gobierno o de gestión de TI no son acordes con las particularidades de las entidades o empresas supervisadas.

✓ Criterios de calificación de los procesos de evaluación

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



- ✓ Cuáles categorías de las funciones de la seguridad cibernética establecidas en el anexo 4 de los lineamientos generales del reglamento resultan adecuadas para evaluar su gestión de riesgos de seguridad cibernética.

- ✓ Diseño e implementación de 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.

Referencia.
Art.42

Auditoría externa de TI

Auditorías externas de TI aplicadas de conformidad con el Marco de prácticas profesionales de auditoría de Tecnologías de Información (ITAF) de ISACA.

Las Superintendencias, según los riesgos identificados, podrán solicitar auditorías externas de TI para los proveedores de bienes y servicios de TI críticos.

Referencia.
Art. 46,47,48

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

- ✓ Cumplir con lo dispuesto en el Reglamento General de Auditores Externos, Acuerdo CONASSIF 1-10, para la contratación de las auditorías externas de TI.

Auditoría externa de TI

- Productos de la auditoría externa de TI
- Presentación de resultados
- Reporte de supervisión
- Inadmisibilidad de los productos
- Plan de acción
- Prórrogas

Referencia.
Art. 52,54,55

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.

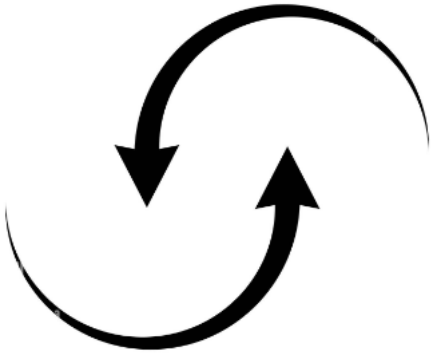
La secuencia y los plazos de las auditorías externas iniciadas con base en el Acuerdo CONASSIF 5-17 no serán interrumpidos por la transición a las modificaciones del presente reglamento.

1

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.

2

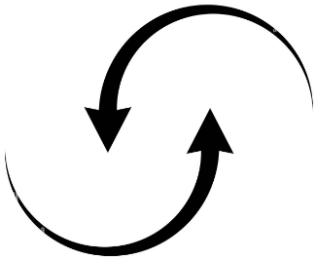


Disposiciones transitorias

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.

3



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

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

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

b) Contratos vigentes: Continúan según lo acordado entre las partes. Las disposiciones aplicarán en caso de renovación del servicio y cuando deban suscribir nuevos contratos y acuerdos de nivel de servicio. En todo caso, dicho plazo no podrá exceder los doce meses a partir de la entrada en vigor del presente reglamento.

4

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:

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

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:

La SUGESE podrá requerir a las Sociedades Corredoras de Seguros, la primera auditoría externa de TI a partir del enero del 2027.

Lineamientos Generales

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

Pautas para la implementación del modelo de clasificación de los activos de información, del impacto potencial en caso de presentarse una brecha de seguridad de la información, así como el acceso y uso de los datos y los activos de información.

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.

Esquemas de clasificación de incidentes de incidentes de seguridad cibernética y sus categorías de impacto.

Tipos, plazos y formatos de los informes de comunicación de incidentes de 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

Estimado señor:

El Consejo Nacional de Supervisión del Sistema Financiero, en los artículos 4 y 5 de las actas de las sesiones 1834-2023 y 1835-2023, celebradas el 20 de noviembre del 2023,

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 quince 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 SUGEVAL Superintendencia General de Valores SUPEN Superintendencia de Pensiones SUGESE

Circular Externa
29 de noviembre de 2023
SGF-3127-2023
A80/0- 2.396
SP-1412-2023
SGS-C-0047-2023
SGF-PUBLICO

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

Muchas gracias

CONASSIF

SUGESE

SUPEN
Superintendencia de Pensiones

SUGEF
Superintendencia General de Entidades Financieras
COSTA RICA

SUGEVAL