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

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

- Fondos complementarios creados por leyes especiales o convenciones colectivas

Asunto: Envío en consulta de la modificación integral a los Lineamientos Generales del Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17.

Las superintendencias adscritas al Consejo Nacional de Supervisión del Sistema Financiero.

Considerando,

1. Que el Consejo Nacional de Supervisión del Sistema Financiero, mediante los artículos 6 y 5 de las actas de las sesiones 1853-2024 y 1854-2024, celebradas el 16 de abril del 2024, aprobó el envío en consulta de la modificación integral del Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17.
2. Que, como complemento a la modificación indicada en el considerando anterior, las autoridades de supervisión han realizado una modificación integral a los lineamientos generales del Acuerdo CONASSIF 5-17, con el objetivo de hacer operativa la citada modificación.
3. Que, El inciso 2) del artículo 361 Ley General de la Administración Pública, Ley 6227, establece que se concederá a las entidades representativas de intereses de carácter general o corporativo afectados por la disposición, la oportunidad de exponer su parecer.

Disponen en firme:

Remitir en consulta, al sistema financiero nacional, cámaras, gremios que los representen y a la Asociación Costarricense de Auditores en Informática**, la propuesta de** modificación integral a los Lineamientos Generales del Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17**, de conformidad con el texto que se incluye a continuación y** en el entendido que, en un plazo máximo de **diez (10) 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.

Sin detrimento de lo anterior, las entidades consultadas pueden presentar de manera consolidada sus observaciones y comentarios a través de los gremios y cámaras que les representan. Asimismo, el correo electrónico normativaenconsulta@sugef.fi.cr será utilizado **únicamente** como mecanismo de notificación sobre la completitud de dicho formulario, respecto del texto que a continuación se transcribe:

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

"Resolución
XX de abril del 2024
XXXX-2024
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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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

Considerando,

1. *Que el Consejo Nacional de Supervisión del Sistema Financiero, mediante el artículo X de la sesión XXXX-2024 del XX de mayo del 2024, aprobó el Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24, publicado en el Alcance N. XX del diario oficial La Gaceta N. XX del X de mayo del 2024.*
2. *Que 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.*
3. *Que, 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.*

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:

1. *Alguna de las entidades o empresas supervisadas preste los servicios de TI a otras entidades o empresas de su mismo grupo o conglomerado financiero.*
2. *Se implementan de forma centralizada las siguientes funciones:*

    a) Aprobación de los objetivos e indicadores estratégicos de TI.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

b) Aprobación de las políticas y procedimientos de TI.

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

d) Gestión de los bienes y servicios de TI tercerizados.

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

f) Establecimiento de estructuras y funciones de gobierno, gestión y control de TI.

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

3. *Plazo de respuesta de las solicitudes de permiso para tipificar la gestión de TI como corporativa:*

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 para etiquetar los activos de información y los datos

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

Objetivo: *Establecer las pautas para la implementación del modelo de clasificación del etiquetado de los activos de información y los datos con base en la clasificación de su acceso y uso según su nivel de confidencialidad.*

1. Clasificación del etiquetado de los activos de información y datos

a) Las entidades y empresas supervisadas, como parte de sus políticas sobre gestión de activos, definirán la clasificación y etiquetado de los activos de información y los datos 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]

[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.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 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

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. 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 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.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

viii. Necesidad del mínimo conocimiento.

ix. Accesos con privilegio mínimo.

x. Segregación y separación de funciones.

xi. Seguridad por diseño o por defecto.

xii. Encriptación de datos en reposo y en tránsito.

xiii. Autenticación con múltiples factores.

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 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.

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

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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 en términos de utilidad*
- *4.4 Descripción de resultados 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*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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 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
ii. 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:

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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.*

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.

3. *Considera la evaluación del estado actual de la capacidad de respuesta a incidentes, incluyendo actividades tales como: encuestas al Órgano de Dirección, Alta Gerencia, encargados de las áreas de TI, autoevaluaciones o evaluaciones y auditorías externas.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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:*

    a) Respuesta del incidente a nivel técnico
        i. En primera instancia, se mitigará su impacto, luego, se eliminarán 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 del 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.

[5] Guías esenciales que capacita 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.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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

c) Respuesta del 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 otras.

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, tales como los siguientes:

a) Gestionar las lecciones aprendidas que permitan mejorar los controles de la entidad o empresa supervisada.
b) Recolectar los datos para el histórico de incidentes.
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

a. 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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

Sección XIX. Lineamientos relacionados con la clasificación 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.*
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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

Clasificación	*Tipo de incidente*	*Descripción práctica*
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, se tomarán en cuenta los siguientes niveles de impacto:

Propiedad de seguridad de la información	*Nivel de impacto / Descripción*		
	Bajo	*Moderado*	*Alto*
Confidencialidad	*La divulgación no autorizada 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 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 divulgación 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.*
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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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. Asimismo, 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 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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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:

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. Cronogramas*
  - *a. Cronograma inicial*
- *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 X1X 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

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. Cronogramas
a. Cronograma inicial
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 X1X 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. Avance de la contención, mitigación y recuperación del incidente
a. Cronogramas
i. Cronograma con porcentaje de seguimiento
ii. Detalle de desviaciones o de riesgos identificados en el cumplimiento de los cronogramas
b. Resumen de las acciones por realizar para:
i. Contención del incidente
ii. Descripción de las actividades ejecutadas
iii. Mitigación del incidente
iv. Descripción de las actividades ejecutadas
v. Recuperación de los sistemas afectados
vi. Descripción de las actividades ejecutadas
vii. Cualquier otro aspecto que la entidad o empresa supervisada considere necesario revelar.

c) Formato del Informe post actividades del incidente

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. Cronogramas
a. Cronograma inicial
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 X1X 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. Avance de la contención, mitigación y recuperación del incidente
a. Cronogramas
i. Cronograma con porcentaje de seguimiento
ii. Detalle de desviaciones o de riesgos identificados en el cumplimiento de los cronogramas
b. Resumen de las acciones por realizar para:
i. Contención del incidente
ii. Descripción de las actividades ejecutadas
iii. Mitigación del incidente
iv. Descripción de las actividades ejecutadas
v. Recuperación de los sistemas afectados
vi. Descripción de las actividades ejecutadas
vii. Cualquier otro aspecto que la entidad o empresa supervisada considere necesario revelar.
6. Informes técnicos

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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 informó el incidente?
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, las direcciones IP y la función
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 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 del reporte histórico de los incidentes de seguridad de la información y seguridad cibernética

Objetivo: *Definir el contenido del reporte histórico de incidentes de seguridad de la información y seguridad cibernética.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

1. Contenido del reporte histórico de incidentes de seguridad de la información y seguridad cibernética

a) El reporte histórico 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.

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:

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

El perfil tecnológico será remitido contra requerimiento expreso de SUGESE en un plazo no mayor a quince 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
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
vi. 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:

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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, realizando pruebas y preparando/resumiendo 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*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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 veinte 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

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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 calificación 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 se realizará por medio de los canales oficiales de comunicación de cada Superintendencia.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

10. Contenido mínimo de la presentación de los resultados de la auditoría externa de TI y las personas que se requiere que asistan

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.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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 plazos y 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 plazos y 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

Los procesos de evaluación del marco de gobierno y gestión de TI aplicables en el momento de la solicitud de la auditoría externa de TI son los siguientes:

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*	*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.*

ID	*Aspectos del marco de gobierno de TI*	*Descripción*	*Propósito*
		objetivos de la entidad o empresa supervisada, a un coste óptimo.	
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*	*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.*

ID	*Aspectos del marco de gestión de TI*	*Descripción*	*Propósito*
		proporcionan externamente, para permitir una respuesta confiable, también ágil y eficiente a los objetivos estratégicos.	
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 tecnologías ya establecidas y por la innovación de procesos organizacionales y de TI. Influenciar la planificación estratégica y las decisiones de arquitectura organizacional.*	*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.*
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*	*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.*

ID	*Aspectos del marco de gestión de TI*	*Descripción*	*Propósito*
		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.	
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*	*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*
		monitorización de los productos y servicios de tecnología e 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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

ID	*Aspectos del marco de gestión de TI*	*Descripción*	*Propósito*
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 procesos de negocio, aplicaciones, información/datos, infraestructura y servicios.*	*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.*
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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

ID	*Aspectos del marco de gestión de TI*	*Descripción*	*Propósito*
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 auditando esta información, y actualizando el repositorio de configuración*	*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.*
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*	*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*

ID	*Aspectos del marco de gestión de TI*	*Descripción*	*Propósito*
		como concluir con una revisión post-implementación.	*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*	*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.*

ID	*Aspectos del marco de gestión de TI*	*Descripción*	*Propósito*
		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.	
2.32	*Gestionar la monitorización del rendimiento y la conformidad*	*Recopilar, validar y evaluar las metas y métricas de alineamiento de la entidad o empresa 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.*	*Proporcionar transparencia en el rendimiento y la conformidad e impulsar la consecución de las metas.*
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

Los procesos de evaluación de la gestión de TI aplicables en el momento de la solicitud de la auditoría externa de TI, para las entidades supervisadas a las que les aplican las disposiciones de regulación proporcional, son los siguientes:

1. Entidades supervisadas por SUGEF

1. *Entidades supervisadas por SUGEF sujetas a la Regulación proporcional para cooperativas de ahorro y crédito, Acuerdo SUGEF 25-23: en el momento de la solicitud de la auditoría externa de TI, aplicarán los siguientes procesos para evaluar la gestión de TI (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. Entidades supervisadas por SUGESE

2. *Las Sociedades Corredoras de Seguros: en el momento de la solicitud de la auditoría externa de TI, aplicarán los siguientes procesos para evaluar la gestión de TI (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*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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.

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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.*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4

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
Tomás Soley Pérez
Superintendente General de Valores
Superintendente General de Seguros

Firmado Digitalmente
Adrián Pacheco Umaña
Superintendente a.i.
Superintendencia de Pensiones

Firmado Digitalmente
José Armando Fallas Martínez
Superintendente a.i.
Superintendencia General de Entidades Financieras

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*

Tel: (506) 2243-3891
Fax: (506) 2243-4582
Apdo: 10058-1000
Barrio Tournón: Avenida 17 Calle 3ª, piso 4