Auditoría Interna

3 de mayo de 2023
AI-As-007-2023

Señor
Alberto López Chaves
Gerente General

Asunto: *Servicio de asesoría sobre la gestión de riesgos institucional y supervisión continua del sistema de control interno.*

Estimado señor:

La Auditoría en cumplimiento del Plan Anual de Trabajo, revisa los procesos de gestión de riesgo institucional y de supervisión continua del sistema de control interno, con una perspectiva de mejores prácticas obteniéndose las oportunidades de mejora siguientes:

Condiciones y criterios

1. Proceso de gestión de riesgo

1.1 El Modelo de Gestión de Riesgos Institucional -MOGERI[1]- no incluye los aspectos siguientes:

- Las estrategias, objetivos y procesos institucionales para la implementación de la estrategia del SEVRI, **-**punto 3.1.1 Política de valoración del riesgo institucional[2], inciso a) Objetivo y compromiso**-**.

- Las funciones y responsabilidades de los participantes en la gestión del riesgo institucional.

[1] Aprobado en sesión ordinaria virtual N°6143, artículo 5, inciso VII, celebrada el 26/10/2020 -Acuerdo de Junta Directiva SJD-435-2020 del 30/10/2020-.
[2] 3. Establecimiento del SEVRI. 3.1 Marco Orientador

- La Alta Dirección no ha definido y declarado el apetito de riesgo -tipos de riesgo y nivel de riesgo- que la Institución está dispuesta a asumir para el logro de los objetivos.

- El glosario con definiciones, conceptos y abreviaturas que defina, explique y uniforme los términos usados en el proceso de gestión de riesgos.

La Ley General de Control Interno[3] -LGCI-, artículo 14, inciso a) y las Normas de Control Interno para el Sector Público -NCISP- norma 3.3, establecen que, se debe identificar y analizar los riesgos relevantes asociados, a la misión, la visión, objetivos y las metas institucionales.

Las Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional -Directrices SEVRI- [4], directriz "3.3 Ambiente de apoyo", inciso d), estipula que, las responsabilidades deben estar definidas claramente en relación con el SEVRI.

Las directrices SEVRI, apartado 3.2, Marco Orientador e Informe de Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño -COSO ERM[5]- principio 7, indican que, se deben establecer los parámetros de aceptabilidad de los riesgos, mediante un perfil de riesgos que contemple al menos el nivel de riesgo que la entidad está dispuesta a asumir -apetito de riesgo-[6], la variación aceptable de dicho nivel -tolerancia al riesgo- y el nivel máximo de riesgo que la entidad puede asumir -capacidad de riesgo-. [6]

Las NCISP, norma 1.4 a), indica que, la Administración debe contemplar, entre otros asuntos, la definición de criterios que brinden una orientación básica para la instauración y el funcionamiento de los componentes orgánicos y funcionales -componentes- del SCI.

1.2 Portafolio de riesgos

El portafolio -inventario estructura- de riesgos presentado en el MOGERI- no incluye los riesgos siguientes:

[3] Ley 8292.
[4] D-3-2005-CO-DFOE.
[5] Committee of Sponsoring Organizations of the Treadway Commission, Junio de 2017.
[6] Informe Nro. DFOE-BIS-IF-00005-2021, 23 de junio, 2021.

Auditoría Interna

- Riesgos asociados a factores ESG[7] -medioambientales, responsabilidad social y gobernanza- dada la importancia de estos en la misión, visión y objetivos estratégicos institucionales.

- Los riesgos de fraude no están clasificados por tipos, ejemplo: fraude, sobornos y conflicto de intereses.

COSO ERM y la guía para la Gestión del riesgo empresarial[8], indican que la Institución debe contar con un inventario donde se registran los riesgos que pueden afectar a la Institución, este inventario debe ofrecer categorías comunes y definiciones estándar a través de las cuales los riesgos pueden describirse y analizarse.

El Modelo Institucional del Sistema de Control Interno -MISCI-, principio 8, establece que, la Institución debe considerar la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos y tener en cuenta los distintos tipos de fraude.

El Manual de Buenas Prácticas de Lucha Contra la Corrupción de la OLACEFS, establece que, los objetivos del control interno se enfocan en lograr la eficacia y eficiencia de las operaciones estatales, la fiabilidad de la información financiera y el cumplimiento de las leyes y normas que sean aplicables. Para fortalecer los esquemas de control interno y consolidar un sistema eficaz, es necesario considerar el análisis de los riesgos de corrupción. Además, el citado Manual destaca la necesidad de generar reportes de administración de riesgos por departamentos, mejorar las metodologías de identificación de riesgos de fraude y generar constantes auto-evaluaciones del control interno[9].

[7] Gestión del riesgo empresarial -Aplicación de la gestión del riesgo empresarial a los riesgos relacionados con factores medioambientales, sociales y de gobierno-

[8] Aplicación de la gestión del riesgo empresarial a los riesgos relacionados con factores medioambientales, sociales y de gobierno.

[9] https://olacefs.com/manual-de-buenas-practicas-de-lucha-contra-la-corrupcion-espanol (página 51-53).

Auditoría Interna

1.3 Etapas del proceso de gestión de riesgos -ver apéndice 1-

a) Identificación de riesgos:

El procedimiento para la identificación de riesgos del ICT no establece una secuencia o sucesión ordenada de las actividades**.**

COSO ERM[10] ordena las actividades para realizar la identificación de riesgos de la siguiente forma:

1. Tomar en cuenta, al menos, los siguientes insumos necesarios para identificar los eventos:
   - Estrategias -Misión y Visión-
   - Objetivos
   - Apetito de riesgo, tolerancia y capacidad.
   - Contexto interno y externo.
   - Portafolio de riesgos.

2. Seleccionar la estrategia, objetivo, proceso, actividad, meta sobre el cual se realizará la gestión de riesgos
3. Analizar el contexto institucional para conocer los factores internos y externos que influyen en las estrategias y objetivos institucionales.
4. Revisar el portafolio -inventario-estructura- de riesgos y verificar que los riesgos existentes siguen siendo aplicables y relevantes.
5. Identificar riesgos nuevos, emergentes y cambiantes que afecten el cumplimiento de las estrategias - objetivos. Si se identifican nuevos riesgos se deben incluir en el portafolio de riesgos.
6. Identificar posibles riesgos de fraude.
7. Redacción del riesgo: evento-causa-consecuencia.

b) Evaluación de la gravedad[11] -análisis y evaluación del riesgo-[12]

- El procedimiento análisis del riesgo del ICT[13], es omiso en las actividades a realizar para determinar el riesgo inherente y el riesgo residual.

[10] Principios 6, 7, 8 y 9
[11] COSO ERM Principios 11 y 12
[12] MOGERI segunda y tercera actividad
[13] Segunda actividad

- El procedimiento de evaluación del riesgo del ICT[14], es omiso en las actividades y criterios para priorizar la gravedad de los riesgos.

La Guía Metodológica para la Elaboración de Procedimientos[15], en el punto 2.4.4.7, establece que, la descripción del procedimiento es la secuencia de actividades constitutivas del procedimiento y se representa en forma de prosa, además debe indicar, entre otras, la descripción narrativa de las actividades secuenciales para desarrollar el procedimiento. Asimismo, la información debe ser completa -toda la necesaria para ejecutarla-; concisa -solo información necesaria-; concreta -ajustarse a los métodos en uso, aprobados, o que seguirán usándose a partir de la elaboración del manual-.

Las Directrices SEVRI estipulan que los riesgos analizados deberán ser priorizados de acuerdo con criterios institucionales, igualmente, COSO ERM, Principio 12, indica que se debe establecer los criterios para priorizar los riesgos para dotar la toma de decisiones de información adecuada sobre las respuestas al riesgo y para optimizar la asignación de recursos. La priorización tiene en cuenta la gravedad del riesgo en comparación con el apetito al riesgo y sugiere los siguientes criterios: adaptabilidad, complejidad, velocidad, persistencia, recuperación.

c) Respuestas ante los riesgos[16] -administración de riesgos[17]-

Los conceptos para evaluar y seleccionar las medidas para la administración de cada riesgo a saber: “atención, modificación, transferencia, prevención y retención” no están definidos, por lo tanto, no permite una estandarización de criterios[18].

Las NCISP, norma 1.4 a), indica que, la Administración debe contemplar la definición de criterios que brinden una orientación básica para la instauración y el funcionamiento de los componentes orgánicos y funcionales -componentes- del SCI.

[14] Tercera actividad
[15] Emitida por la Unidad de Planificación -Setiembre 2018-
[16] COSO ERM Principio 13
[17] MOGERI cuarta actividad
[18] Procedimiento: Cuarta Actividad -Administración de riesgos-

COSO ERM, principio 13, tiene definidos conceptualmente los siguientes criterios para evaluar y seleccionar las medidas para la administración de cada riesgo, que son: aceptar, evitar, perseguir, reducir y compartir.

1.4 Sistema utilizado para la evaluación de los riesgos

El sistema de información para la gestión de riesgos institucionales -SYNERGY- no tiene inmerso dentro de su estructura actividades que se establecen en el MOGERI, según detalle:

- No tiene la información de los parámetros establecidos para la capacidad y la tolerancia sobre los objetivos, definida en el MOGERI.

- La redacción de la causa y consecuencia son parte de la etapa de identificación de riesgos; no obstante, en el SYNERGY esta actividad se realiza en la etapa de análisis y evaluación.

- No permite documentar la evaluación de los siguientes criterios, que según el MOGERI se deben considerar para seleccionar la medida de administración de cada riesgo:
  - Análisis costo beneficio
  - Capacidad e idoneidad para la ejecución
  - Cumplimiento intereses público y resguardo
  - Viabilidad Jurídica, técnica y operacional de las opciones
  - Resultado esperado

- No permite llevar un análisis histórico de los riesgos institucionales, con:
  - El historial del seguimiento y supervisión continua de los riesgos19,
  - La evaluación y ajustes de los objetivos y metas institucionales,
  - El cumplimiento de objetivos de acuerdo con la capacidad y tolerancia, y
  - La valoración del riesgo por parte de los responsables.

- No incluye la parametrización para el establecimiento del apetito y priorización del riesgo.

[19] G-1143-2022

- No permite emitir informes del resultado del perfil de riesgo institucional por categorías de riesgos, gravedad del riesgo, interdependencias de riesgos, cómo afectan el cumplimiento de la estrategia y objetivos. -mapa de riesgos-

Las Directrices SEVRI, directriz 3.6, establece que, la herramienta deberá contar con un sistema de registros de información que permita el análisis histórico de los riesgos institucionales y de los factores asociados a dichos riesgos.

Las NCISP 5.6.1 y 5.6.3, Calidad de la información –confiabilidad y utilidad indican que, la Institución debe asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios, de modo que se encuentre libre de errores, defectos u omisiones y posea características de pertinencia, relevancia, suficiencia y presentación adecuada.

2. Supervisión continua del sistema de control interno

La Auditoría emite el servicio preventivo AI-Ad-14-2022, donde comunica oportunidades de mejora sobre la supervisión continua y fueron atendidas por la Gerencia mediante la Circular G-1143-2022, pero ésta no se aplica de forma estandarizada.

La LGCI establece como un deber del jerarca y de los titulares subordinados que los funcionarios responsabilizados realicen continuamente las acciones de control y prevención en el curso de las operaciones normales integradas a tales acciones[20].

Las NCISP disponen que, las actividades de seguimiento del SCI, deben incluir la comprobación durante el curso normal de las operaciones, del cumplimiento de las actividades de control incorporadas en los procesos[21] y que los funcionarios dentro de su labor cotidiana, deben observar el funcionamiento del SCI[22] con el fin de determinar las desviaciones en su efectividad, e informarlas oportunamente a las instancias correspondientes.[23]

[20] Artículo 17, Seguimiento del sistema de control interno, inciso a)

[21] 6.3 Actividades de seguimiento del SCI inciso a)

[22] Componentes SCI: Ambiente de control, Valoración de Riesgo, Actividades de Control, Sistemas de Información y Seguimiento.

[23] 6.3.1 Seguimiento continuo del SCI

Auditoría Interna

El MISCI[24] establece que, la Gerencia debe ejercer la supervisión del SCI, entre otras, mediante evaluaciones continuas, definir la frecuencia y el alcance considerando el ritmo de cambio en la Institución y en los procesos de negocio, éstas constituyen operaciones rutinarias, que se integran en los procesos y se realizan en tiempo real, para responder ante un entorno cambiante.

Causas

Las condiciones determinadas en los puntos anteriores se presentan debido a que:

- El MOGERI no contiene las actividades de control para garantizar eficientemente el proceso de gestión de riesgos y supervisión continua institucional por la forma en que está estructurado y desarrollado.

- Las modificaciones realizadas en el MOGERI no han sido incluidas en el SYNERGY.

- La UPI como unidad encargada del establecimiento y gestión de riesgos, no se actualiza con las últimas tendencias o marcos que existen, como, por ejemplo: COSO ERM y COSO ESG. La Auditoría en agosto 2022 emite el Informe AI-C-07-2022 y recomienda *"Gestionar capacitación a los colaboradores de la UPI sobre COSO ERM*".

- No se realiza una inducción y no hay un procedimiento estandarizado para realizar la supervisión continua que instruye la Gerencia mediante la Circular G-1143-2022

- La Administración no cuenta con un programa para la sensibilización de la cultura institucional sobre la gestión de riesgos y supervisión continua.

Efectos

Los riesgos a que puede verse expuesta la Institución por las condiciones determinadas son:

[24] Principio 16, Punto Enfoque 16.1, documento probatorio

Auditoría Interna

- Que se puedan materializar riesgos importantes o estratégicos y que incidan en el cumplimento de los objetivos del ICT establecidos en el PEI y en el PNT.
- La institución no disponga en forma oportuna de información sobre riesgos relevantes asociados al logro de la estrategia institucional y de los objetivos propuestos para la toma de decisiones.
- Que no se cuente con un enfoque moderno para la gestión y supervisión del riesgo.
- Que no se cuente con una herramienta sistemática que permita monitorear los cambios significativos e impida reaccionar de forma oportuna y adecuada en la atención de los riesgos.
- Que no se realicen evaluaciones continuas de las operaciones rutinarias que están integradas en los procesos relevantes en tiempo real.
- Inducir a error a los funcionarios que realizan la gestión de riesgos por no contar con criterios uniformes y procedimientos claros.
- Que se afecte negativamente la rendición de cuentas por no estar definidos los roles y responsabilidades de los funcionarios que participan en la gestión de riesgos.

La Auditoría en el ejercicio de la función de asesoría suministra criterios, observaciones, opiniones y advertencias resultado de los procesos de control y fiscalización y, son comunicados a la Administración como insumos para que le permitan tomar decisiones más informadas y ajustadas al ordenamiento jurídico y técnico y con ello fortalecer el sistema de control interno y coadyuvar con el logro de los objetivos institucionales.

La Ley Orgánica, artículo 32, establece que, la Gerencia es el responsable del eficiente y correcto funcionamiento administrativo de la Institución y debe ejercer las funciones inherentes a su condición de administrador general y jefe superior del Instituto, vigilando la organización, funcionamiento y coordinación de todas sus dependencias y la observación de las leyes, reglamentos y resoluciones de la Junta Directiva, razón por la cual, se comunica lo determinado sobre la gestión del riesgo y supervisión continua, con el propósito que se tomen las acciones pertinentes para que se subsanen las causas identificadas y administrar al menos los riesgos determinados en este servicio preventivo sobre la gestión de riesgos y supervisión continua.

Auditoría Interna

Se solicita a la Gerencia, informar a esta Auditoría Interna dentro de los próximos diez días hábiles, sobre las decisiones y acciones tomadas en relación con esta asesoría, a efecto de determinar lo procedente.

.

El servicio de asesoría se realiza con fundamento en las competencias conferidas a la Auditoría Interna en la Ley Orgánica del ICT, artículos 33 y 35, la Ley General de Control Interno, artículo 22, inciso d), las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, norma 1.1.4

Atentamente,

ROMEL ALVAREZ NAVARRO (FIRMA)

Firmado digitalmente por ROMEL ALVAREZ NAVARRO (FIRMA)
Fecha: 2023.05.03 08:46:30 -06'00'

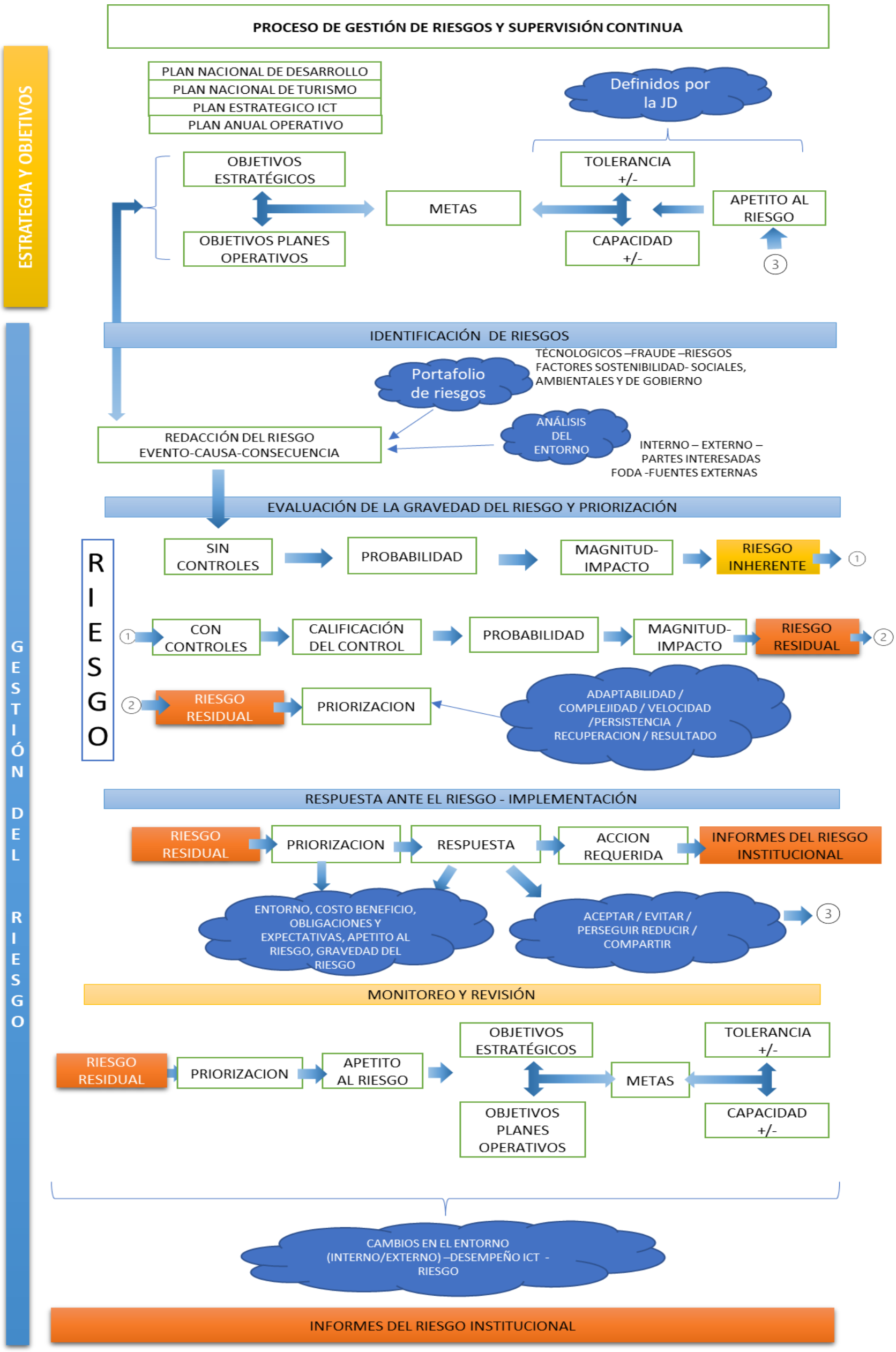
Rómel Álvarez Navarro
Auditor Interno a.i.

C. Sr. Víctor Quesada Rodríguez
Unidad Planificación Institucional
Comité de Auditoría y Riesgos
Consecutivo

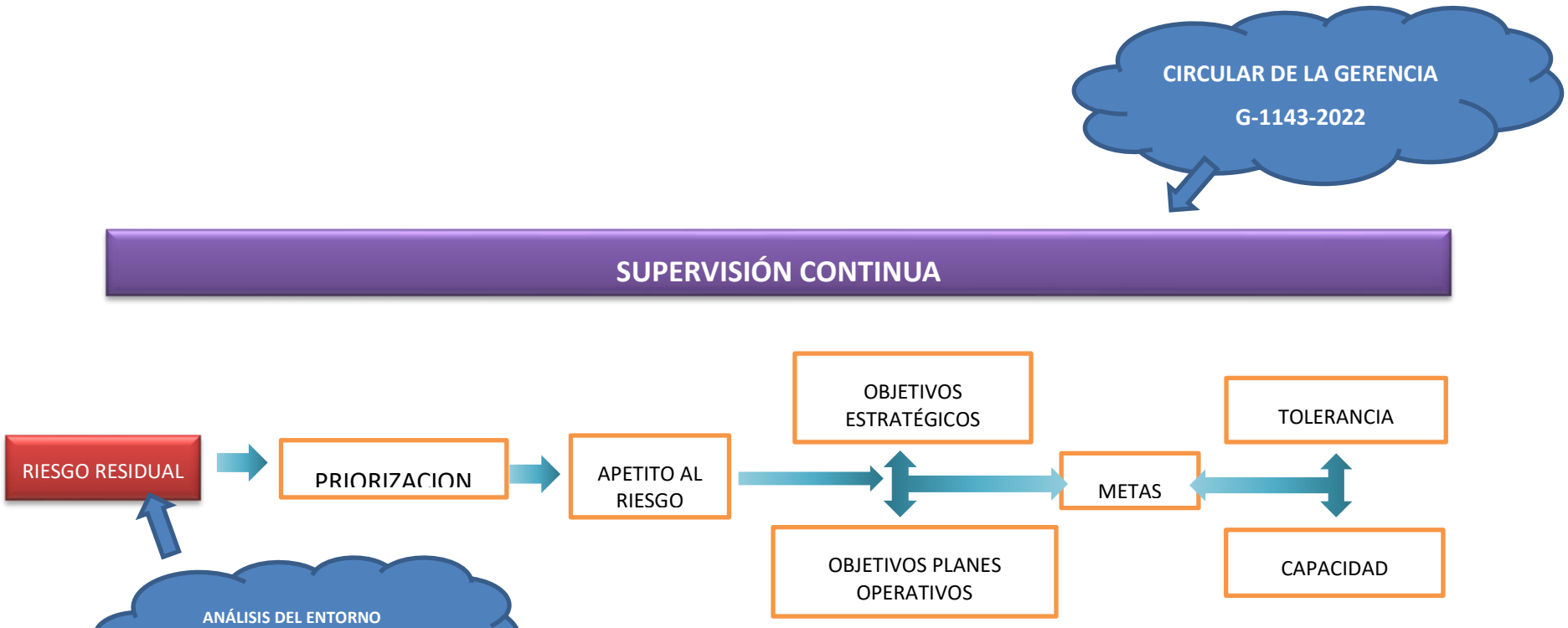
RAN/kbm-src

Auditoría Interna

Apéndice 1
Proceso de Gestión de Riesgos y supervisión continua



Auditoría Interna



FECHA	RESPONSABLE DEL REGISTRO	OBSERVACIONES SOBRE EL ENTONO QUE AFECTAN LA ESTRATEGIA/ OBJETIVO/META	% DE CUMPLIMIENTO META A LA FECHA DEL REGISTRO	AFECTACIÓN DE LA META DEL OBJETIVO	ACCIÓN REQUERIDA					
					CAMBIO DE LOS CONTROLES	SE REQUIERE CAMBIO EN LA META DE ESTRATEGIA/ OBJETIVO/META	ACTIVIDADES / TAREAS	RESPONSABLE	RECURSOS	FECHA DE IMPLEMENTACIÓN
20/1/2023		AFECTACIÓN DEL TIPO DE CAMBIO	20%	NO	No requiere	No aplica	No aplica	No aplica	No aplica	No aplica

Dirección: Costado Este del Puente Juan Pablo II, La Uruca
Teléfonos: 2299-5708 2299-5700
Correo electrónico: auditoriainterna@ict.go.cr web: www.ict.go.cr
Apartado Postal: 777-1000 San José, Costa Rica