**AUDITORÍA INTERNA**
**INSTITUTO NACIONAL DE SEGUROS**

# AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA APLICACIÓN DEL SISTEMA ESPECÍFICO DE VALORACIÓN DE RIESGOS (SEVRI) EN EL INS

**IA-038-2022**
**06 DE DICIEMBRE DE 2022**

## RESUMEN EJECUTIVO

El presente informe contiene el resultado de la auditoría de carácter especial sobre la aplicación a nivel institucional de las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI) emitidas por la Contraloría General de la República, que se realizó como parte del Plan Anual de Trabajo de la Auditoría para el 2022.

El objetivo general del estudio fue verificar el cumplimiento de dichas Directrices, mediante la revisión de la implementación de los componentes definidos en el SEVRI para este fin, tomando en consideración que se debe establecer y mantener en funcionamiento dicho Sistema, conforme lo establece la Ley General de Control Interno, con el propósito de contribuir a su fortalecimiento.

Para lograr el objetivo planteado, se desarrollaron pruebas de efectividad para cada una de las áreas en revisión, según los lineamientos establecidos en estas Directrices, así como, la normativa complementaria creada para gestionar el marco integral de riesgos institucional.

De acuerdo con los resultados obtenidos, se determinó la existencia de varios aspectos sujetos de mejora y/o debilidades de control, concretamente lo siguiente:

- ✓ Falta de actualización de la matriz de aplicación de las valoraciones de riesgo operativo por parte de la Dirección de Riesgos Corporativa, según la Metodología General para la gestión integral de riesgo operativo, que fue aprobada en sesión de Junta Directiva N° 9701-VII del 31-01-2022.
- ✓ Necesidad de estandarizar los nombres de los riesgos identificados, según su clasificación, en la normativa interna.
- ✓ Se debe reforzar el proceso de documentación de las valoraciones de riesgo operativo y el seguimiento de los riesgos identificados, de acuerdo con las medidas establecidas para la administración de estos, por parte de la Dirección de Riesgos Corporativa.
- ✓ Se requiere la revisión integral de: los indicadores de riesgo de cumplimiento, los umbrales de riesgo definidos por parte de la Dirección Cumplimiento Normativo Corporativa y sobre el tratamiento para la administración de los riesgos de cumplimiento identificados.
- ✓ Falta de claridad en las referencias incluidas en la Metodología para determinar el nivel de riesgo y priorización de normativas de la Dirección Cumplimiento Normativo Corporativa.
- ✓ Falta de actualización de los objetivos de la Dirección de Cumplimiento Normativo Corporativa en el Manual de Organización y funciones, y sobre las actividades de seguimiento dentro de la Política de Cumplimiento Normativo.

De acuerdo con las situaciones expuestas, se formulan las recomendaciones que a criterio de esta Auditoría deben ponerse en práctica para fomentar el fortalecimiento del sistema de gestión de riesgos institucional, como parte del mejoramiento del marco de gobierno corporativo.

## TABLA DE CONTENIDOS



### Tablas

**IA-038-2022**
**06 de diciembre de 2022**

# I. INTRODUCCIÓN

## A. Origen del Estudio

De conformidad con el Plan Anual de Trabajo de Auditoría para el 2022, se realizó la auditoría de carácter especial sobre la aplicación a nivel institucional de las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI) de la Contraloría General de la República.

## B. Objetivo General

Verificar el cumplimiento de la aplicación del Sistema Específico de Valoración de Riesgos Institucional (SEVRI) en el INS, mediante la revisión de los procedimientos, actividades e informes presentados por parte de la Dirección de Riesgos Corporativa, con el fin de determinar el cumplimiento de la normativa aplicable.

## C. Naturaleza y Alcance

Se realizó una auditoría de carácter especial, sobre la evaluación del marco para la aplicación de las Directrices Generales citadas en el INS, durante el periodo 2022 y se extendió en aquellos casos en los que se consideró pertinente ahondar.

## D. Metodología

El estudio se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público y demás normativa aplicable al ejercicio de la auditoría interna, las Directrices Generales citadas, según la información proporcionada o generada por la Dirección de Riesgos Corporativa y Dirección de Cumplimiento Normativo Corporativa.

La información se procesó mediante análisis documental, entrevistas y consultas a los funcionarios encargados de los procesos y actividades.

## E. Marco Normativo

- ✓ Ley General de Control Interno N° 8292.
- ✓ Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI).
- ✓ Acuerdo CONASSIF 04-16. Reglamento sobre Gobierno Corporativo (anteriormente Acuerdo SUGEF 16-16).
- ✓ Acuerdo SUGESE 09-17. Reglamento sobre los Sistemas de Gestión de Riesgos y Control Interno aplicables a Entidades Aseguradoras y Reaseguradoras.
- ✓ Normas de Control Interno para el Sector Público.
- ✓ Política de Gestión Integral de Riesgos.
- ✓ Política de Cumplimiento Normativo.

- ✓ Política del Instituto Nacional de Seguros sobre control interno.
- ✓ Metodología general para la gestión integral de riesgos operativos.
- ✓ Metodología de los principales riesgos de cumplimiento.
- ✓ Metodología para determinar el nivel de riesgo y priorización de normativas.
- ✓ Manual Técnico para completar “Base de incumplimientos” CNS-MAT-0003.

### F. Comunicación de Resultados

La debilidad de control y situaciones sujetas a mejora que se exponen en este informe fueron presentadas mediante reunión efectuada el 06/12/2022, por medio de la herramienta Microsoft Teams, a los señores: Lic. Álvaro Vega Vega, Jefe de Dirección de Riesgos Corporativa, Lic. Jairo Jonathan Dávila Castañeda y Lic. Esteban Chavarría Olmedo, ambos Subjefes de la Dirección de Riesgos Corporativa y Licda. Wendy Azofeifa Chacón, Líder de procesos de Cumplimiento Normativo, como representante delegada por la Lcda. Yirlany González Calderón, Jefa de la Dirección Cumplimiento Normativo Corporativa, quienes manifestaron su conformidad con los resultados y recomendaciones que se formulan, lo cual quedo consignado en el Anexo N°1. Acta de comunicación de resultados.

## II. RESULTADOS

### A. Análisis de aspectos a cargo de la Dirección de Riesgos Corporativa.

La Dirección de Riesgos Corporativa es la responsable de desarrollar, coordinar e implementar el proceso de gestión integral de riesgos, razón por la cual, la verificación del cumplimiento de las Directrices Generales para el establecimiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI), se basó en la revisión del marco y los lineamientos creados para este propósito.

Al respecto, se observó que por medio de la Declaratoria de Apetito de Riesgo (DAR) se determina la cantidad de riesgo que el INS está dispuesto a aceptar en la búsqueda de su misión, visión y/o objetivos. La misma fue aprobada por la Junta Directiva mediante acuerdo N°9733-VII del 20-07-2022, según la capacidad de riesgo establecida y la estrategia de gestión de riesgos institucional, en concordancia con los objetivos estratégicos y del negocio. Además, por medio de las herramientas detalladas en la Política de Gestión de Riesgos Institucional se gestionan los demás riesgos (principalmente el riesgo operativo y las diferentes categorías de este).

La Declaratoria de Apetito de Riesgo corresponde a un conjunto de indicadores para los cuales el negocio (unidades organizacionales del INS) trasladan información y la Dirección de Riesgos Corporativa la analiza, esto con el fin de definir si se plantean o no como indicadores, gestionándose por medio de la construcción de estos, y donde los resultados del cálculo se miden según los umbrales definidos, mientras que las etapas del proceso de valoración de riesgos (identificación, análisis, evaluación, administración y revisión de los riesgos institucionales) se aplican por medio de la implementación de las metodologías que se han creado al efecto.

**IA-038-2022**
**06 de diciembre de 2022**

La Dirección de Riesgos Corporativa emite diversos informes producto de su gestión, que son presentados al Comité de Riesgos Corporativo, Junta Directiva o algún otro ente, según el tema y la periodicidad requerida, entre los que se encuentran:

- ✓ Informes mensuales y trimestrales: contiene el detalle de los resultados del cálculo de los indicadores de la Declaratoria de Apetito de Riesgo y de las acciones desarrolladas para controlar los indicadores que se encuentran por fuera del umbral, y el análisis del estado de los diferentes riesgos gestionados u estudios especiales realizados.
- ✓ Informe anual de autoevaluación de riesgo y solvencia: corresponde al análisis de los resultados sobre los riesgos que se gestionaron durante un año.
- ✓ Informes de riesgo operativo: corresponde a los resultados del proceso de valoración del riesgo operativo de forma general, así como, emite un informe por cada proceso o dependencia valorada.

Producto de la revisión, se determinaron las siguientes debilidades de control y/o situaciones sujetas de mejora:

## 1. Debilidades de control observadas en relación con el marco institucional en materia de gestión de riesgos.

### 1.1. Sobre la Metodología General para la gestión integral de riesgo operativo.

Para la aplicación de la Metodología general para la gestión integral de riesgo operativo, aprobada en acuerdo de Junta Directiva N° 9701-VII del 31-01-2022, se observa de forma general, que se sigue utilizando la matriz de valoración de riesgos operativos anterior a dicha aprobación, asimismo, se identificó el siguiente aspecto:

- ✓ En la Metodología se definieron los “impactos” para la determinación de los riesgos inherentes que podrían presentarse, con sus respectivos criterios, por medio de una escala que va de muy baja a extremas pérdidas económicas, sin hacerse la indicación de un rango cuantificable para dicha pérdida. No obstante, se observa que la columna de “impacto” no se encuentra alineada con esta escala, debido a que la información en la matriz de aplicación se presenta en términos económicos (es decir, se mide en millones de colones).

La situación descrita obedece a que la Dirección de Riesgos Corporativa no ha actualizado aún la herramienta (matriz) para la valoración de riesgo operativo, con respecto a los parámetros definidos en la Metodología general para la gestión integral de riesgos operativos, lo que puede ocasionar que se estén generando resultados incorrectos, de acuerdo con los nuevos parámetros establecidos y que se puedan materializar los riesgos de desviaciones en la gestión de riesgos y de calidad de la información.

Al respecto, resulta importante indicar, lo que se establece en las Directrices Generales para el establecimiento y funcionamiento del SEVRI, en su punto 4.4. Análisis de riesgos, en lo que

respecta a que el análisis de riesgos debe realizarse de acuerdo con los criterios institucionales establecidos, para este caso, según lo definido en la Metodología General para la gestión integral de riesgo operativo.

## 2. Aspectos sujetos de mejora observados sobre el marco institucional en materia de gestión de riesgos.

### 2.1. Sobre la Política de Gestión Integral de Riesgos.

De acuerdo con la revisión de la Política de Gestión Integral de Riesgos vigente, se determinaron las siguientes situaciones sujetas de mejora:

- ✓ En el apartado 11.3 Declaración de Apetito de Riesgo*,* se indica que el perfil de riesgo de cada categoría se clasificará en términos de: “Bajo”, “Moderado”, “Alto” y “Extremo” (cuatro niveles), no obstante, la DAR cuenta con cinco niveles de riesgo, concretamente los siguientes: “Muy bajo”, “Bajo”, “Moderado”, “Alto” y “Extremo”. Asimismo, los parámetros de aceptabilidad establecidos en esta sección, en relación con estos últimos aspectos, se encuentran desactualizados.

  Además, se menciona que el apetito por riesgo operativo aprobado es de “Bajo-Moderado”, de acuerdo con las escalas de frecuencia e impacto económico, que se exponen en Anexo N°2. Mapa de calificación y umbrales de riesgos operativos, de esa Política. No obstante, este nivel y anexo se encuentran desactualizados, debido a que contienen información relacionada con la Metodología de Autoevaluación de Riesgo Operativo y no se refieren a la Metodología general para la gestión integral de riesgos operativos.

- ✓ La Política de Gestión Integral de Riesgos menciona de forma general a la autoevaluación de riesgo o Metodología de Autoevaluación de Riesgo Operativo, sin embargo, con la actualización realizada, lo correcto sería hacer referencia a la Metodología general para la gestión integral de riesgos operativos.

- ✓ En el apartado 19.1 Metodologías, herramientas y modelos de medición*,* correspondiente a las Políticas para la gestión del riesgo reputacional, se indica que uno de los medios de medición corresponde a la Herramienta “Tablero de KRI’s”, no obstante, el riesgo reputacional no está contemplado como eje dentro de la DAR, siendo el tablero parte de la Declaratoria.

En relación con lo anterior, la Dirección de Riesgos Corporativa se encuentra trabajando en tres documentos normativos distintos para complementar la Política de Gestión Integral de Riesgos, a saber: Marco de Gestión Integral de Riesgos, Política de Gestión Integral de Riesgos y Disposiciones complementarias a la Política de Gestión Integral de Riesgos, donde se incluye la actualización de los puntos anteriores, no obstante, los documentos no han sido debidamente aprobados por las instancias correspondientes.

Asimismo, resulta necesario que se tomen en consideración las siguientes situaciones, como parte de la actualización y/o modificación de los diferentes cuerpos normativos:

- ✓ Estandarización de los nombres de los riesgos a utilizar, según se expone en la siguiente tabla:

**Tabla 1. Detalle de riesgos utilizados en la normativa interna.**

| Declaración de Apetito de Riesgo (Ejes) | Política de Gestión Integral de Riesgos | Propuesta de actualización del Marco de Gestión Integral de Riesgos | |
|---|---|---|---|
| Riesgo financiero | Riesgo financiero | Riesgo financiero | Riesgo de liquidez |
| | | | Riesgo de mercado |
| | | | Riesgo de crédito |
| Riesgos técnicos | Riesgos técnicos de seguros | Riesgos técnicos de seguros | |
| Riesgo de crédito | Riesgo de crédito | Corresponde a una subcategoría de riesgos financieros | |
| Riesgo operativo | Riesgo operativo | Riesgos no financieros | Riesgo legal |
| | | | Riesgo reputacional |
| | | | Riesgo de tecnologías de información |
| | | | Riesgo de seguridad de la información y ciberseguridad |
| | | | Riesgo de fraude interno |
| | | | Riesgos de nuevos productos y su remozamiento. |
| | | | Riesgos de proveedores |
| Riesgo de legitimación de capitales | Riesgo de legitimación de capitales y financiamiento al terrorismo | La clasificación no existe dentro de la actualización. | |
| Riesgo tecnológico | Riesgo tecnológico | Corresponde a una subcategoría de riesgos no financieros | |
| No existe el eje dentro de la DAR. | Riesgo de liquidez | Corresponde a una subcategoría de riesgos financieros | |

| | | |
|---|---|---|
| No existe el eje dentro de la DAR. | Riesgos de mercado | Corresponde a una subcategoría de riesgos financieros |
| No existe el eje dentro de la DAR. | Riesgo reputacional | Corresponde a una subcategoría de riesgos no financieros |
| No existe el eje dentro de la DAR. | Riesgo de grupo | Riesgo de conglomerado |
| No existe el eje dentro de la DAR. | No existe dentro de Política vigente. | Riesgo de proyectos |

Fuente: *Elaboración de la Auditoría Interna con base en la información recopilada y analizada.*

Se observa en la tabla anterior, que se elimina la categoría del Riesgo de Legitimación de Capitales y Financiamiento al Terrorismo (Riesgo de legitimación de capitales), dentro de la propuesta de documentos del Marco de Gestión Integral de Riesgos.

Lo anterior, se da debido a que la Dirección de Riesgos Corporativa no ha identificado aún la necesidad de estandarizar los nombres de los riesgos y la clasificación de riesgos realizada entre la normativa interna relacionada y de incluir la categoría de riesgo de legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva (LC/FT/FPADM), según se denomina correctamente, cuya gestión está a cargo de la Oficialía de Cumplimiento Corporativa y que se evalúa conforme a la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades Conexas, legitimación de capitales y financiamiento al terrorismo, Ley N° 7786, sus reformas, y normativa conexa; lo cual puede ocasionar que se presenten confusiones u omisiones a la hora de presentar y analizar la información, lo que a su vez incide en los riesgos de calidad de la información y de informes y reportes.

Al respecto, se debe de tomar en cuenta lo establecido en las Normas de Control Interno para el Sector Público, en los numerales 4.4 Exigencia de confiabilidad y oportunidad de la información, 4.5 Garantía de eficiencia y eficacia de las operaciones y 5.6 Calidad de la información, en lo que respecta a la necesidad de contar con normativa que sea congruente.

### 2.2. Sobre el seguimiento de los riesgos identificados, de acuerdo con las medidas establecidas para su administración.

En la Política de Gestión Integral de Riesgos se establecen los lineamientos generales para el seguimiento de los planes de acción, que se generen producto de las medidas establecidas para la administración de los riesgos, no obstante, la Dirección de Riesgos Corporativa se encuentra trabajando en la modificación de esta política, según se indicó anteriormente.

Al respecto, producto de la revisión de la propuesta de normativa, se determinó que no se establecen lineamientos generales sobre el proceso de seguimiento a los planes de acción que se generen como parte de la gestión de riesgos, como se indica en la política vigente.

Aunado a lo anterior, se localizó en la carpeta compartida de la Dirección de Riesgos Corporativa, específicamente en la siguiente ruta: *H:\Dirección de Riesgos\2- Operativo\3 Valoraciones de Riesgo\1 Operativos\4 Macroprocesos y Procesos 2021\2 Asuntos varios,* el archivo denominado "Matriz Planes de Acción VRO 2021.xls"*,* correspondiente al control sobre el seguimiento de los planes de acción que se han generado a la fecha, donde se observan las siguientes situaciones:

- ✓ Un evento de riesgo identificado, calificado como "moderado", pendiente de atención.
- ✓ Las fechas de seguimiento corresponden únicamente a febrero y marzo de 2022, sin evidenciarse monitoreos posteriores.
- ✓ No se brinda detalle de la referencia del informe o valoración de riesgo operativo que genera el seguimiento (oficio o informe), año de la valoración y/o las correspondientes observaciones sobre la verificación realizada o documentación relacionada, ni de las actividades realizadas producto del tratamiento del riesgo identificado.
- ✓ No se identificó en los informes, la información relacionada con el estado de los correspondientes planes de acción, que son generados por medio de las valoraciones de riesgo operativo.

Lo anterior, se da por la omisión de parte de la Dirección de Riesgos Corporativa, de establecer dentro de la normativa que se encuentran actualizando, aquellos lineamientos específicos para el seguimiento y revisión de los riesgos identificados, así como, por la falta de un control que le permita conocer de forma integral la gestión de revisión y seguimiento de los planes de acción.

Lo observado, expone a la Institución a los riesgos de cumplimiento, de informes y reportes, así como de calidad de la información, debido a que no se cuenta con la totalidad de la información y su estado actual, asimismo, se puede ver afectado el riesgo de desviaciones en la gestión de riesgos y de toma de decisiones.

Al respecto, se debe destacar lo que indican las Directrices Generales para el establecimiento y funcionamiento del SEVRI, en el punto 4.6. Revisión de riesgos, en lo que respecta al seguimiento de los riesgos identificados y que este debe ejecutarse de forma continua, con el fin de que sirva para ajustar las medidas establecidas para la administración de los riesgos identificados.

### 2.3. Documentación relacionada con las valoraciones de riesgo operativo.

La información correspondiente a las valoraciones de riesgo operativo se encuentra en una carpeta compartida de la Dirección de Riesgos Corporativa, de acuerdo con la siguiente ruta: *H:\Dirección de Riesgos\2- Operativo\3 Valoraciones de Riesgo\1 Operativos.*

Al respecto, se determinó que la documentación incluida para cada una de las valoraciones realizadas no es uniforme y no presenta un orden determinado, lo cual se da por la ausencia o falta de aplicación de lineamientos específicos para documentar todo el proceso de valoración de riesgos.

Lo observado expone a la Institución al riesgo de cumplimiento y al riesgo de calidad de la información, al no contarse con toda la documentación compilada para su consulta y revisión, como parte del proceso de gestión de riesgos.

Lo anterior, para cumplir con lo que se establece en las Directrices Generales para el establecimiento y funcionamiento del SEVRI, en el punto 4.7. Documentación de riesgos, donde se indica que los registros deben ser accesibles, comprensibles y completos y que la documentación se realice de forma continua, oportuna y confiable. Asimismo, en la sección 1. Glosario, se define "documentación de riesgos" como: "…*a la actividad permanente del proceso de valoración del riesgo que consiste en el registro y la sistematización de información asociada con los riesgos...",* entendiéndose esto último, al ordenamiento de esta.

**B. Análisis de aspectos a cargo de la Dirección Cumplimiento Normativo Corporativa.**

Como parte de la gestión de riesgos institucional, corresponde a la Dirección Cumplimiento Normativo Corporativa (DCNC) gestionar el riesgo de cumplimiento, por lo que se revisó el marco creado para este fin. Al respecto, se identificó que este riesgo se gestiona aplicando las etapas de valoración de riesgos (identificación, análisis, evaluación, administración y revisión de los riesgos institucionales), por medio de la implementación de las metodologías que se han diseñado y aplicado para este propósito.

Asimismo, esta Dirección emite informes semestrales sobre el avance en el cumplimiento de su plan anual de trabajo, incluyendo los resultados sobre las valoraciones de riesgo de cumplimiento realizadas, los cuales van dirigidos a la Junta Directiva, Comité de Riesgos Corporativo, Comité de Cumplimiento Corporativo e informes individuales sobre los resultados de las valoraciones dirigidas al dueño del proceso evaluado.

Producto de la revisión, se determinaron las siguientes situaciones de mejora:

**1. Aspectos de mejora observados sobre el marco institucional en materia de gestión de riesgos.**

**1.1. Sobre los indicadores de riesgo de cumplimiento y los umbrales de riesgo definidos.**

Dentro de la Declaratoria de Apetito de Riesgo (DAR), en el eje de riesgo operativo, se establecen los siguientes indicadores relacionados a la gestión de cumplimiento normativo (CN):

- ✓ 45. Actividades de cultura de CN ejecutadas en el trimestre /Acciones ejecutadas / Actividades de cultura de CN definidas en el Plan Anual de Trabajo 2022 de DCN.
- ✓ 46. Evaluaciones de riesgo de CN realizadas en el trimestre / Evaluaciones de riesgo de CN definidas en el plan Anual de Trabajo 2022 de DCN de Accidentes Individuales.
- ✓ 47. Estudios especiales de CN finalizadas en el trimestre / Estudios especiales definidos en el Plan Anual de Trabajo 2022 de DCN.

- ✓ 48. Informes periódicos de CN finalizados en el trimestre / Informes periódicos de CN definidos en el Plan Anual de Trabajo 2022 de DCN.

Como se observa, estos indicadores no miden el riesgo de cumplimiento como tal, sino las actividades entorno a este, de forma similar a los indicadores que se incluyen en un determinado Plan Anual Operativo (PAO). De acuerdo con el análisis de la información, se determinó que estos indicadores se crearon de esta forma, debido a que no se contaba con los datos necesarios para su construcción dentro de la Herramienta para Gestión de Cumplimiento Normativo (HECUM).

Por otra parte, en esta herramienta se incluyen varios indicadores del riesgo de cumplimiento, los cuales constituyen una de las fuentes necesarias para estimar el perfil de riesgo de cumplimiento y para poder realizar una gestión eficaz del mismo, los cuales no son congruentes con los indicadores establecidos en la DAR.

Adicionalmente, los indicadores incluidos en el HECUM solo cuentan con cuatro niveles de riesgo, a saber: “Bajo”, “Moderado”, “Alto” y “Extremo”, por lo que tampoco se encuentran alineados con los umbrales aprobados para la DAR y consecuentemente, el proceso definido en el Sistema de Gestión de Calidad (CNS-PRO-0002 Gestión de cumplimiento normativo), solo contempla esos mismos cuatro niveles de riesgo.

Cabe señalar que los umbrales propuestos por la Dirección Cumplimiento Normativo Corporativa, mediante oficio DCN-00110-2021 del 20-04-2021, aprobados por la Junta Directiva del INS mediante sesión N° 9651-VII del 17-05-2021, cuentan con cinco niveles de riesgo (“Muy bajo”, “Bajo”, “Moderado”, “Alto” y “Extremo”). No obstante, los valores fueron ajustados, debido a que el HECUM solo tiene cuatro niveles parametrizados. Aunado a que se incluyen en esta, tres indicadores que no fueron presentados ante la Junta Directiva para su respectiva aprobación, según se muestra en la siguiente tabla:

**Tabla 2. Indicadores de riesgo incluidos en el HECUM aprobados por Junta Directiva.**

| | | | Umbrales de riesgo incluidos en HECUM | | | | | | Umbrales de riesgo según DCN-00110-2021 del 20-04-2021 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Denominación del indicador | abr-22 | Nivel de riesgo | Bajo | Moderado | Alto | | Extremo | Muy bajo | Bajo | Moderado | Alto | | Extremo |
| 1 | Cantidad de normativas externas que vencen al mes siguiente | 0 | Bajo | 2 | 5 | 7 | > | 7 | No estaba incluido dentro del oficio | | | | | |
| 2 | Nuevas normativas externas sin planes de acción | 0 | Bajo | 0 | 1 | 2 | > | 2 | | | | | | |
| 3 | Nuevas normativas externas con planes de acción vencidos o retrasado | 0 | Bajo | 0 | 1 | 2 | > | 2 | | | | | | |
| 4 | Riesgos potenciales de cumplimiento normativo fuera del apetito de riesgo | 0 | Bajo | 1 | 2 | 3 | > | 3 | 0 | 1 | 2 | 3 | > | 3 |
| 5 | Riesgos potenciales sobre normativas externas por fuera del apetito de riesgo con planes vencidos o sin planes de acción | 0 | Bajo | 1 | 2 | 3 | > | 3 | 0 | 1 | 2 | 3 | > | 3 |
| 6 | Incumplimientos normativos (internos y externos) | 107 | Extremo | 30 | 60 | 90 | > | 90 | 30 | 45 | 60 | 90 | > | 90 |
| 7 | Incumplimientos de normativas externas con planes vencidos o sin planes de acción | 0 | Bajo | 10 | 30 | 40 | > | 40 | 10 | 20 | 30 | 40 | > | 40 |
| 8 | Cantidad de incumplimientos sujetos a posibles sanciones | 84 | Extremo | 5 | 10 | 20 | > | 20 | 0 | 5 | 10 | 20 | > | 20 |
| 9 | Cantidad de incumplimientos (internos y externos) de alta antigüedad | 102 | Extremo | 5 | 10 | 20 | > | 20 | 0 | 5 | 10 | 20 | > | 20 |
| 10 | Monto potencial de multa (en colones) sobre patrimonio | 0 | Bajo | 0,01 | 2,0% | 5,0% | > | 5,0% | 1,0% | 2,0% | 4,0% | 5,0% | > | 5,0% |
| 11 | Monto de multa efectiva (en colones) sobre patrimonio | 0 | Bajo | 0,01 | 2,0% | 5,0% | > | 5,0% | 1,0% | 2,0% | 4,0% | 5,0% | > | 5,0% |

*Fuente: Elaboración de la Auditoría Interna con base en la información recopilada y analizada.*

Por otra parte, por medio de la aplicación de la Metodología de los principales riesgos de cumplimiento, se obtienen mapas de calor del riesgo inherente y residual, con una escala de calificación de cinco niveles (“Muy bajo”, “Bajo”, “Moderado”, “Alto” y “Extremo”), lo cual no es concordante con lo indicado anteriormente para la calificación de normativas en el HECUM y lo establecido en el Manual Técnico para completar “Base de incumplimientos”.

Lo anterior, no ha sido unificado o estandarizado, debido a que la Dirección Cumplimiento Normativo Corporativa mantiene la meta de contar en el año 2023, con un sistema GRC (Gobierno, Riesgo y Cumplimiento), que integre las actividades y funciones de gobierno corporativo, la administración de riesgos y las responsabilidades de cumplimiento, por lo que no se ha considerado necesario alinear el HECUM con los parámetros de gestión de riesgos establecidos. Tampoco se ha valorado la oportunidad de contar con información actualizada para ser utilizada como base para el nuevo sistema, al momento de su adquisición.

Asimismo, se observa que en el HECUM no se han incluido los datos generados por medio de las valoraciones de riesgo de cumplimiento, por lo que para el cálculo de los indicadores no se cuenta con toda la información necesaria. Esto se da debido a que la Dirección Cumplimiento Normativo Corporativa indica que no cuenta con los recursos para actualizar la herramienta con esa información; situación que ha sido reiterada en diversos informes emitidos por esta Auditoría (Ref. Informes IA-017-2021 del 23-04-2021, IA-001-2022 del 19-01-2022 e IA-012-2022 del 01-04-2022).

Lo observado expone a la Institución a riesgos de desviaciones en la gestión de riesgos y de toma de decisiones, al no contarse con indicadores que permitan determinar el nivel de riesgo de cumplimiento, por la falta de alineamiento y estandarización de los niveles de riesgo establecidos en las herramientas utilizadas, generando información incorrecta, y a riesgos de calidad la información y de informes y reportes, sobre los resultados de esa gestión.

Al respecto, es importante señalar lo que se indica en el Reglamento sobre los Sistemas de Gestión de Riesgos y de Control Interno Aplicables a Entidades Aseguradoras y Reaseguradoras, en su artículo 3. Definiciones, en lo que respecta al concepto de apetito de riesgo, el establecimiento de niveles de riesgo aceptables según las Directrices Generales para el establecimiento y funcionamiento del SEVRI (inciso 3.2. Marco orientador) y con lo indicado en el numeral 5.6. Calidad de la Información de las Normas de control interno para el Sector Público, sobre la exigencia de confiabilidad, oportunidad y calidad de la información.

### 1.2. Sobre la Metodología para determinar el nivel de riesgo y priorización de normativas.

En la Metodología para determinar el nivel de riesgo y priorización de normativas, específicamente en los numerales 1. Objetivo y 3. Nivel de riesgo / prioridad de las obligaciones de cumplimiento (normativas externas e internas), hacen referencia a la última columna de la “Estructura y definición campos inventario normativas internas y externas” y del “Inventario de normativas externas e internas”, pero no se menciona el archivo concreto al que corresponde dicha referencia.

Lo anterior, se origina por la omisión por parte de la Dirección Cumplimiento Normativo Corporativa, de incluir dicha referencia en la metodología a utilizar, para facilitar su correcta ubicación al usuario.

Asimismo, se observa que la Metodología hace referencia a los niveles de riesgo “Bajo”, “Moderado”, “Alto” y “Extremo”, para la categorización del nivel de riesgo de acuerdo con la clasificación de la normativa, lo cual no está alineado con los umbrales de la gestión de riesgo de la Dirección de Riesgos Corporativa (cinco niveles) y con la Metodología de los principales riesgos de cumplimiento de la Dirección Cumplimiento Normativo Corporativa.

Además, no se visualiza la existencia de criterios para el tratamiento de riesgos, de acuerdo con el nivel de riesgo que se obtenga, es decir, que permitan seleccionar la o las medidas para la administración de cada riesgo identificado, dirigidas a la atención, modificación, transferencia y prevención de riesgos.

Aunado a lo anterior, dentro del archivo de seguimiento de los planes de acción, se incluye la totalidad de los incumplimientos identificados desde un nivel de “Moderado” o mayor a este, de acuerdo con el apetito de riesgo institucional y no se presenta dentro del control, el detalle del incumplimiento al que se le da seguimiento y los responsables de la atención de los respectivos planes de acción.

Del mismo modo, se identifica la ausencia de lineamientos para la aplicación de la metodología relacionada con los niveles de riesgo aprobados y con la práctica administrativa de utilizar el nivel de apetito aprobado en la DAR, para gestionar los riesgos de cumplimiento, y para que se incluyan los detalles sobre el incumplimiento identificado en el control de seguimiento.

La falta de referencias claras en las herramientas utilizadas puede ocasionar que se generen riesgos de eficacia por información desactualizada o que se implementen procesos de forma inadecuada y que no se cuente con toda la información necesaria para la determinación de los planes de acción y su respectivo seguimiento; además esto puede generar eventuales riesgos de desviaciones en la gestión de riesgos, por la aplicación de un tratamiento que no corresponda, al no realizarse un análisis integral sobre los niveles de riesgo a utilizar y su tolerancia establecida.

En ese sentido, resulta importante considerar lo que las Directrices Generales para el establecimiento y funcionamiento del SEVRI señalan, en cuanto a los parámetros de aceptabilidad de riesgo y el análisis y evaluación de riesgos, así como el punto 4.6. Revisión de riesgos, en lo que respecta al seguimiento a los riesgos identificados.

### 1.3. Actualización de normativa interna.

El objetivo general y los objetivos específicos del Manual de Organización y Funciones de la Dirección Cumplimiento Normativo Corporativa hacen referencia al tema de control interno, cuya función fue traslada a la Dirección de Planificación, concretamente al Departamento de Control

Interno, en atención al acuerdo de Junta Directiva N° 9717 del 18-04-2022. Asimismo, se incluye el objetivo específico "*Gestionar la cultura organizacional del INS, mediante la implementación de un conjunto articulado de acciones permanentes que permitan una incorporación transversal de la ética y los valores"**,*** cuya gestión no es competencia de la Dirección Cumplimiento Normativo Corporativa, sino que está a cargo del Comité Corporativo de Ética, Conducta y Derechos Humanos del Grupo INS y de la Subdirección de Cultura y Talento, según el tema que corresponda.

Por otra parte, en la Política de Cumplimiento Normativo, apartado 9. Informes de resultados, se indica que se emiten mensualmente reportes a los órganos competentes, incluyendo la Alta Administración y trimestralmente a la Junta Directiva. No obstante, en la práctica se emite un informe de labores semestral y se presentan los informes de valoración de riesgos de cumplimiento, según se vayan generando.

Al respecto, la Dirección Cumplimiento Normativo Corporativa se encuentra en proceso de actualización de dicha normativa, no obstante, inicialmente definió los objetivos y pautas sobre las actividades de seguimiento, tomando en consideración las condiciones e información con la que contaba en ese momento, por lo que es necesario realizar las modificaciones correspondientes, según la realidad y la práctica actual, ya que mantener la información de esta forma puede propiciar la materialización de riesgos de calidad de la información y de eficacia por información desactualizada, así como, el riesgo de cumplimiento por no realizarse actividades que se encuentran establecidas en dicha normativa, lo que consecuentemente afecta el riesgo de informes y reportes.

Al respecto, se debe tomar en cuenta lo señalado en las Normas de control interno para el Sector Público, en su numeral 5.6. Calidad de la información.

### C. Aspectos positivos y de conformidad con la normativa.

La Dirección de Riesgos Corporativa cuenta con un equipo multidisciplinario para la gestión de riesgos institucionales, el cual se maneja mediante la creación e implementación de un marco de gestión integral de riesgos, donde se establecen los elementos y componentes que van a gobernar las acciones que se deben llevar a cabo, conforme se define en la Política de Gestión Integral de Riesgos, el cual se encuentra en proceso de ajuste y actualización (Marco, Política y las Disposiciones complementarias), según se indicó anteriormente.

Dentro de las herramientas que la Dirección de Riesgos Corporativa ha desarrollado están las metodologías y los modelos de riesgo, métodos, políticas y procedimientos para el manejo de dicha gestión; además, cuenta con el apoyo del Comité de Riesgos Corporativo para la validación de los instrumentos propuestos por esta, previa presentación y aprobación de la Junta Directiva, lo cual refuerza el marco de gestión integral de riesgos.

Asimismo, dentro de la estructura organizacional se cuenta con la Dirección de Cumplimiento Normativo Corporativa, que posee un marco desarrollado e implementado para la administración integral del riesgo de cumplimiento, que de igual forma genera informes para el Comité de

Riesgos Corporativo, Comité de Cumplimiento Corporativo y Junta Directiva, como parte de la gobernanza.

Adicionalmente, dentro del marco de gestión de riesgos se utiliza como referencia, no solo las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI), sino, que, para la gobernanza de los riesgos, de forma complementaria se toman en consideración los acuerdos CONASSIF 04-16. Reglamento sobre Gobierno Corporativo (anteriormente Acuerdo SUGEF 16-16) y SUGESE 09-17. Reglamento sobre los Sistemas de Gestión de Riesgos y Control Interno aplicables a Entidades Aseguradoras y Reaseguradoras.

Por otra parte, ambas Direcciones (DRC y DCNC), promueven la adecuada gestión de riesgos y el proceso de culturización para robustecer la gestión, con el fin de obtener mejores resultados y atender las debilidades que se puedan ir presentando, así como, para crear una mayor conciencia sobre los riesgos institucionales.

## III. CONCLUSIONES

Se verificó el cumplimiento de la aplicación del Sistema Específico de Valoración de Riesgos Institucional (SEVRI) en el INS, determinándose que se presentan dos tratamientos complementarios entre sí para gestionar los riesgos institucionales: a) el correspondiente a los riesgos más relevantes que se gestionan mediante la Declaratoria de Apetito de Riesgos (DAR) y b) los que se gestionan mediante otras herramientas o metodologías, tales como el riesgo operativo y las diferentes categorías de este.

A pesar de la diferenciación identificada, se corroboró que se atienden de forma razonable los lineamientos establecidos en la Directrices Generales para el establecimiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), especialmente por medio de la Política de Gestión Integral de Riesgos.

Asimismo, se determinó que la gestión de riesgos se ve complementada mediante la aplicación de los aspectos normados en el Acuerdo SUGESE 09-17 Reglamento sobre los Sistemas de Gestión de Riesgos y de Control Interno Aplicables a Entidades Aseguradoras y Reaseguradoras y Acuerdo CONASSIF 04-16 Reglamento de Gobierno Corporativo, siendo esta práctica permitida siempre y cuando no se contraponga a lo que se establece en las Directrices citadas, según el artículo 3. Facultad de promulgar normativa técnica sobre control interno**,** de la Ley General de Control Interno (Ley 8292), lo que le permite a la Institución contar con un marco de gestión de riesgo más amplio y robusto.

Aunado a lo anterior, del análisis de la gestión del riesgo de cumplimiento realizada por la Dirección Cumplimiento Normativo Corporativa, se determina que esta cumple de forma razonable con las Directrices; no obstante, esta Auditoria enfatiza que es necesario que se concrete la formalización de la estructura de organización y funciones de esa Dirección, así

como, la asignación final de recursos para su adecuado funcionamiento, con el fin de consolidar el marco de gestión de cumplimiento.

Asimismo, se identificaron varios aspectos sujetos de mejora y/o debilidades de control que deben ser atendidas para continuar robusteciendo la gestión de riesgos institucional.

## IV. RECOMENDACIONES

**Para la Dirección de Riesgos Corporativa:**

**A.1.** Revisar de forma integral la matriz de aplicación de la Metodología General para la gestión integral de riesgo operativo y ajustarla de acuerdo con los parámetros establecidos en esta, brindando especial atención a la escala definida para la valoración del "impacto" para los riesgos inherentes identificados. (II.A.1.1) **Prioridad: Alta.**

**A.2.** Corroborar que dentro de la formalización y aprobación de los documentos normativos relacionados a la gestión de riesgos que se encuentra en proceso, se incorpore al menos lo siguiente:

- ✓ Actualización de la clasificación de los niveles de riesgo (muy bajo, bajo, moderado, alto y extremo) y los parámetros de aceptabilidad de riesgo según lo definido en la Declaratoria de Apetito de Riesgo, del anexo N°2 Mapa de calificación y umbrales de riesgos operativos y del nombre de la Metodología General para la Gestión Integral de Riesgos operativos.
- ✓ Modificación del detalle sobre las metodologías, herramientas y modelos de medición correspondientes al riesgo reputacional. (II.A.2.1) **Prioridad: Baja.**

**A.3.** Revisar y alinear la Declaratoria de Apetito de Riesgo (DAR) y la normativa relacionada (Política de Gestión Integral de Riesgo vigente y disposiciones complementarias propuesta), en lo que se refiere a los nombres y estructura de las clasificaciones de riesgo establecidas dentro del marco de gestión de riesgos, así como, considerar la incorporación del riesgo de legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva (LC/FT/FPADM), como riesgo relevante dentro de esta, con el fin de estandarizar la información. (II.A.2.1) **Prioridad: Baja.**

**A.4.** Contemplar dentro de la actualización del marco normativo de la Dirección de Riesgos Corporativa la incorporación y el establecimiento de los lineamientos específicos para las actividades relacionadas con el seguimiento y revisión de los riesgos identificados, donde se contemple como mínimo los siguientes aspectos:

1. Periodicidad del reporte del avance por parte de los dueños de los procesos.
2. Estructura y forma de reporte (documentación requerida).
3. Periodicidad del monitoreo o seguimiento por parte de la Dirección de Riesgos Corporativa y responsables.

4. Medidas o tratamiento en el caso de incumplimientos de planes de acción por parte de los dueños de los procesos.
5. Periodicidad, informes y reportes por medio de los cuales se va a informar a los sujetos interesados sobre el estado de los riesgos identificados. (II.A.2.2) **Prioridad: Media.**

**A.5**. Diseñar e implementar un control por escrito con el detalle de los riesgos identificados y que requieren de algún tratamiento según los lineamientos establecidos, que contenga como mínimo la siguiente información:

1. Detalle de la referencia del informe o valoración de riesgo que genera el seguimiento (consecutivo del oficio donde se informó), año de la valoración (fecha)
2. Detalle de las actividades a realizar y responsable del plan de acción (dueño del proceso).
3. Observaciones sobre la verificación realizada o documentación relacionada por parte de la Dirección de Riesgos Corporativa.

Asimismo, definir el informe en donde se presentará el detalle sobre el estado y seguimiento de dichas acciones para ser comunicado al Comité de Riesgos Corporativo y a la Junta Directiva. (II.A.2.2) **Prioridad: Media.**

**A.6.** Diseñar e implementar un protocolo o guía por escrito, donde se defina la información total que se debe documentar, producto de las valoraciones de riesgo operativo que realiza la Dirección de Riesgos Corporativa, contemplando además las particularidades de cada valoración (primera, segunda u otra) y el orden que debe llevar, con el fin de contar con registros completos y que el proceso de documentación se realice de forma continua, oportuna y confiable.

Asimismo, hacer extensivo el protocolo o guía establecida para toda valoración de riesgos que se realice. (II.A.2.3) **Prioridad: Media.**

**Para la Dirección Cumplimiento Normativo Corporativa:**

**B.1.** Incorporar en la Herramienta para Gestión de Cumplimiento Normativo (HECUM), principalmente en la base de incumplimientos, la información generada por medio de las valoraciones de riesgo, con el fin de tener información real y actual sobre la gestión de riesgo de cumplimiento, que sirva de base para el cálculo de los indicadores que se creen y para la eventual carga de la información en el sistema GRC (Gobierno, riesgo y cumplimiento), en caso de que se adquiera. (II.B.1.1.) **Prioridad: Alta.**

**B.2.** Valorar la información con la que se cuenta en la actualidad y determinar si con esta, se pueden incorporar indicadores que midan el riesgo de cumplimiento dentro de la Declaratoria de Apetito de Riesgo (DAR), tomando en consideración los indicadores formulados en la Herramienta para Gestión de Cumplimiento Normativo (HECUM), esto con el fin de sustituir los indicadores existentes que miden la gestión de cumplimiento. (II.B.1.1.) **Prioridad: Media.**

**B.3.** Establecida la viabilidad de realizar lo anterior, junto con la Dirección de Riesgos Corporativa coordinar la incorporación formal dentro Declaratoria de Apetito de Riesgo (DAR) de los

indicadores de riesgos definidos, contemplando además la creación del eje de riesgo de cumplimiento y demás información relacionada. (II.B.1.1.) **Prioridad: Media.**

**B.4.** Realizar un análisis técnico e integral para determinar la viabilidad de modificar la Herramienta para Gestión de Cumplimiento Normativo (HECUM), para alinear dicha herramienta con los parámetros de gestión de riesgos establecidos, específicamente lo relacionado a los niveles de riesgo aprobados, considerando que la información contenida en dicha herramienta será la base de información a cargar en el sistema que se adquiera. (II.B.1.1.) **Prioridad: Media.**

**B.5.** Estandarizar los parámetros de gestión de riesgos establecidos, en la normativa interna siguiente:

- ✓ Indicadores aprobados mediante sesión del N° 9651-VII del 17-05-2021 (oficio DCN-00110-2021 del 20-04-2021).
- ✓ Procedimiento CNS-PRO-0002 Gestión de cumplimiento normativo.
- ✓ Metodología de los principales riesgos de cumplimiento.
- ✓ Metodología para determinar el nivel de riesgo y priorización de normativas.
- ✓ CNS-MAT-0003 Manual Técnico para completar “Base de incumplimientos”

Asimismo, efectuar una revisión integral de toda la normativa interna relacionada, con el fin de alinearla entre sí. (II.B.1.1.) **Prioridad: Media.**

**B.6.** Incorporar dentro de la Metodología para determinar el nivel de riesgo y priorización de normativas, la referencia sobre el archivo específico a utilizar, correspondiente a la clasificación de la normativa por nivel de riesgo. (II.B.1.2.) **Prioridad: Baja.**

**B.7.** Establecer dentro de la gestión del riesgo de cumplimiento los parámetros correspondientes a los criterios para el tratamiento de los riesgos identificados, de acuerdo con el nivel de riesgo que se obtenga, es decir, seleccionar la o las medidas pertinentes para la administración de los riesgos identificados (por ejemplo, medidas dirigidas a la atención, modificación, transferencia y prevención de riesgos), con el fin de definir el proceso a seguir para la generación de planes de acción y/o seguimiento de los incumplimientos identificados. (II.B.1.2.) **Prioridad: Alta.**

**B.8.** Incorporar dentro del control de los riesgos identificados y que requieren de algún tratamiento según los lineamientos establecidos, el detalle del incumplimiento identificado y los responsables del plan de acción definido. (II.B.1.2.) **Prioridad: Media.**

**B.9.** Considerar dentro de la actualización de normativa interna que se encuentran realizado, la modificación de los siguientes aspectos:

- ✓ Objetivo general y específicos de la Dirección Cumplimiento Normativo Corporativa en el Manual de Organización y Funciones.
- ✓ Sobre la presentación de informes de resultados de la Política de Cumplimiento Normativo y su periodicidad. (II.B.1.3.) **Prioridad: Media.**

**Hecho por**

LUIS GUILLERMO CASTRO LIZANO (FIRMA)

Firmado digitalmente por LUIS GUILLERMO CASTRO LIZANO (FIRMA)
Fecha: 2022.12.06 14:43:13 -06'00'

Lic. Luis Guillermo Castro Lizano
Auditor I

**Hecho por**

WENDY CHACON VILLALOBOS (FIRMA)

Firmado digitalmente por WENDY CHACON VILLALOBOS (FIRMA)
Fecha: 2022.12.06 14:59:11 -06'00'

Licda. Wendy Chacón Villalobos
Auditor I

**Revisado y aprobado por**

RODRIGO MUÑOZ SOLERA (FIRMA)

Firmado digitalmente por RODRIGO MUÑOZ SOLERA (FIRMA)
Fecha: 2022.12.06 15:03:52 -06'00'

Lic. Rodrigo Muñoz Solera
Jefe de Auditoría Operativa