CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

DT CAIGG N° 70 - Versión 0.4 - 2026

DOCUMENTO TÉCNICO N° 70

Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público

RESENTACIÓN

En cumplimiento de las instrucciones del Presidente de la República, Sr. Gabriel Boric Font, orientadas al fortalecimiento de la Política de Auditoría Interna de Gobierno, el Consejo de Auditoría Interna General de Gobierno (CAIGG), en su calidad de órgano asesor del Supremo Gobierno en auditoría interna, control interno, probidad, gestión de riesgos y gobernanza, presenta el Documento Técnico N° 70, versión 0.4, titulado "Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público".

En este contexto, el Consejo promueve el desarrollo de capacidades institucionales y pone a disposición herramientas técnicas tanto para las unidades de Auditoría Interna como para los gestores públicos responsables de dirigir, coordinar y supervisar los procesos, alineadas con las mejores prácticas nacionales e internacionales.

Esta versión, actualizada conforme a los marcos y estándares vigentes en gestión de riesgos, se concibe como una guía práctica para la implementación, mantención y mejora continua del proceso de gestión de riesgos en los organismos del Estado.

Santiago, marzo de 2026.

Daniella Caldana Fulss
Auditora General de Gobierno

TABLA DE CONTENIDO

RELACIÓN DE ANEXOS

I. INTRODUCCIÓN

En la actualidad un factor fundamental para el éxito de la gestión de una entidad sea pública o privada, la constituye su Gobierno Corporativo. Según la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el Gobierno Corporativo es el sistema por el cual las sociedades del sector público y privado son dirigidas y controladas. La estructura del Gobierno Corporativo especifica la distribución de los derechos y de las responsabilidades entre los diversos actores de la empresa, como, por ejemplo, el consejo de administración, el presidente y los directores, accionistas y otros terceros proveedores de recursos. Sin perjuicio de la definición que quiera aceptarse, el concepto de Gobierno Corporativo considera los esfuerzos por manejar una entidad y mejorar su gestión. Una de las herramientas o mecanismos claves para ello, es la implementación de procesos de gestión de riesgos, que ayuda a las organizaciones al cumplimiento de sus metas estratégicas y operativas y al mejoramiento de sus procesos.

En este sentido, y con la finalidad que las organizaciones gubernamentales mejoren sus procesos y maximicen las posibilidades de cumplir sus metas y objetivos en forma adecuada, es necesario que las organizaciones gubernamentales, mantengan y mejoren las actividades del Proceso de Gestión de Riesgos que se viene desarrollando en la Administración del Estado desde el año 2007. Lo anterior, considerando el levantamiento de procesos de la institución o la revisión de este; la identificación, análisis y valorización de los riesgos críticos y sus controles y, en especial, la formulación de medidas de tratamiento de dichos riesgos.

A contar del año 2022, el enfoque metodológico se basa principalmente, pero no en forma exclusiva, en las Normas Chilenas NCh-ISO 31000:2018, Gestión del Riesgo - Directrices, NCh-ISO 31010:2020, Gestión del Riesgo - Técnicas de Evaluación del Riesgo, NCh- ISO Guía 73:2012, Gestión del Riesgo – Vocabulario y NCh-ISO 31004:2014 Gestión del Riesgo – Orientación para la implementación de ISO 31000. Todas estas, emitidas por el Instituto Nacional de Normalización (INN), organismo que tiene a su cargo el estudio y preparación de las normas técnicas en Chile.

La Norma Chilena NCh-ISO 31000:2018 se estudió a través del Comité Técnico de Gestión de Riesgo del INN, para entregar los principios y orientaciones acerca de la implementación de una gestión del riesgo, como también el establecimiento de su marco de trabajo y sus procesos. Dicha norma es idéntica a la versión en inglés de la Norma Internacional ISO 31000:2018 *Risk Management - Guidelines*.

Sin perjuicio de lo previamente señalado, las organizaciones gubernamentales podrán previa solicitud y aprobación por parte del Consejo de Auditoría Interna General de Gobierno (CAIGG), proponer e implementar, si corresponde, un modelo de gestión de riesgos basado principalmente en la Norma Chilena NCh-ISO 31000:2018 o en otros marcos aceptados, que estén adaptados a las características y particularidades específicas de la organización y a los requerimientos del CAIGG.

En lo que se refiere a la Función de Auditoría Interna, esta tendrá un rol de apoyo para que la dirección pueda alinear el enfoque y las prácticas de gestión de riesgos con la norma NCh-ISO 31000:2018, así como contribuir a mantener estas prácticas alineadas de manera continua. Además, debe proveer aseguramiento a la dirección sobre la efectividad de la gestión de los

riesgos, cuyos resultados en conjunto con las directrices emitidas por el Consejo de Auditoría Interna Gubernamental (CAIGG), servirán para retroalimentar el proceso.
En el presente documento se consolida el marco metodológico y procedimental para la implantación, mantención y actualización del Proceso de Gestión de Riesgos en entidades del sector público, de conformidad con los principios de la norma NCh-ISO 31000:2018, los lineamientos del CAIGG y las buenas prácticas internacionales en gestión de riesgos.

El contenido del documento se estructura en los siguientes capítulos:

I. **Introducción:** Describe los antecedentes, motivaciones y marco legal que sustentan la elaboración de esta guía técnica.

II. **Objetivo General del Documento:** Define el propósito del documento y su aplicabilidad transversal a las entidades públicas.

III. **Marco Metodológico y Conceptual:** Establece los principios rectores, el enfoque normativo y los **conceptos** fundamentales de la gestión de riesgos.

IV. **Componentes Estructurales del Sistema de Gestión de Riesgos:** Presenta los elementos organizacionales esenciales para un sistema robusto de gestión de riesgos, incluyendo roles, gobernanza, cultura y modelo de madurez.

V. **Proceso de Gestión de Riesgos:** Detalla las fases operativas de gestión del riesgo, desde el establecimiento del contexto hasta el registro y reporte, incorporando herramientas, criterios y ejemplos prácticos.

VI. **Gestión de Riesgos de Probidad Administrativa:** Establece los lineamientos técnicos para la identificación, evaluación, tratamiento y monitoreo de los riesgos de probidad administrativa en los órganos de la Administración del Estado, en el marco del Proceso de Gestión de Riesgos

VII. **Mantención y Mejoramiento del Proceso de Gestión de Riesgos:** Define los mecanismos de revisión periódica, auditoría, evaluación de efectividad y retroalimentación organizacional, asegurando la mejora continua del sistema.

VIII. **Referencias Normativas y Bibliográficas:** Compila las fuentes técnicas, normativas y metodológicas utilizadas para la elaboración del presente documento.

Es fundamental destacar que cada organización gubernamental debe implementar un Proceso de Gestión de Riesgos efectivo, que permita identificar y gestionar eventos que puedan comprometer el logro de sus objetivos estratégicos y misión institucional. Para garantizar una gestión sólida, es imprescindible aplicar todas las fases descritas en el presente documento técnico.

Asimismo, el CAIGG podrá requerir periódicamente reportes derivados del Proceso de Gestión de Riesgos. Sin embargo, para cumplir con esta exigencia, las organizaciones gubernamentales deberán ejecutar rigurosamente la metodología establecida en esta directriz. Esto no solo asegura la operatividad de un Proceso de Gestión de Riesgos robusto dentro de la entidad, sino que también garantiza la generación de reportes de alta calidad, diseñados para proporcionar

información relevante y oportuna a la Presidencia de la República. Estos reportes serán clave para coordinar y gestionar de manera efectiva las acciones de los diferentes organismos gubernamentales.

Es necesario recordar que la entrega de información al CAIGG deberá focalizarse en informar sobre los riesgos reales y potenciales para la organización gubernamental, para efectos de hacer una gestión más eficiente, priorizando los temas y materias de mayor relevancia y criticidad en cada proceso o actividad que desempeña.

II. OBJETIVO GENERAL DEL DOCUMENTO

Documentar los procedimientos y facilitar a las organizaciones gubernamentales la implantación y cumplimiento satisfactorio del Proceso de Gestión de Riesgos, así como su mantención y actualización. Para ello, todas las organizaciones deben cumplir al menos los siguientes objetivos:

- Asumir la responsabilidad de la adopción de medidas tendientes a la gestión efectiva de los riesgos, especialmente los de mayor criticidad para la entidad, informando de ello al CAIGG.
- Disponer de los recursos necesarios para la correcta implementación y funcionamiento del Proceso de Gestión de Riesgos en la entidad.

El Proceso de Gestión de Riesgo en las organizaciones gubernamentales, estará regido por el presente documento técnico y por las demás normativas e instrucciones que el CAIGG determine en forma complementaria.

III. MARCO METODOLÓGICO Y CONCEPTUAL

El modelo metodológico para la Gestión de Riesgos en las organizaciones gubernamentales está basado principalmente en las disposiciones de las normas chilenas ya mencionadas anteriormente: NCh-ISO 31000:2018, Gestión del Riesgo - Directrices, NCh-ISO 31010:2020, Gestión del Riesgo - Técnicas de Evaluación del Riesgo, NCh- ISO Guía 73:2012, Gestión del Riesgo – Vocabulario y NCh-ISO 31004:2014 Gestión del Riesgo – Orientación para la implementación de ISO 31000. Todas estas, emitidas por el Instituto Nacional de Normalización (INN), y en menor medida, en otros marcos de gestión de riesgos corporativos[1], como aquella normativa que lo reemplace.

Desde el año 2016, se han integrado elementos conceptuales y metodológicos destinados a identificar y analizar de manera efectiva señales de alerta asociadas a delitos de lavado de activos (LA), financiamiento del terrorismo (FT) y delitos funcionarios (DF). Estas incorporaciones buscan fortalecer los sistemas de gestión de riesgos y mejorar la capacidad de las organizaciones para detectar y prevenir estos riesgos críticos, asegurando así el cumplimiento normativo y la integridad institucional.

Adicionalmente, a partir de esta versión del Documento Técnico N° 70, se han introducido lineamientos y una metodología complementaria para la identificación y tratamiento de riesgos

[1] Marco Gestión de Riesgos Empresariales COSO ERM, Modelo de Capacidad GRC - OCEG, entre otros.

probidad administrativa en las organizaciones gubernamentales. Estas directrices buscan reforzar las capacidades institucionales para prevenir, gestionar y mitigar riesgos que puedan comprometer los principios de probidad, transparencia y ética pública, promoviendo así una gestión alineada con los estándares internacionales y las mejores prácticas en gobernanza y control.

El presente documento se entenderá como el marco técnico de referencia para la implantación, mantención y actualización del Proceso de Gestión de Riesgos en el Estado.

1. Conceptos Generales sobre Riesgos

La Norma NCh-ISO Guía 73:2012 define el riesgo como el efecto de la incertidumbre sobre los objetivos, enfatizando que este se caracteriza comúnmente por la referencia a eventos potenciales, sus consecuencias, o la combinación de ambos. En paralelo, el Marco Integrado de Control Interno – COSO I (Versión 2013) amplía esta perspectiva, definiendo el riesgo como la posibilidad (probabilidad) de que un evento ocurra y afecte negativamente (consecuencia o impacto) el logro de los objetivos.

La evaluación del riesgo se concibe como un proceso dinámico e iterativo que permite identificar y valorar los riesgos en función de su impacto potencial en los objetivos organizacionales. Este análisis debe realizarse considerando los niveles predefinidos de tolerancia al riesgo, lo que permite establecer límites claros para la gestión. De este modo, la evaluación de riesgos se convierte en un pilar fundamental para determinar las estrategias y medidas necesarias para su tratamiento.

Como condición previa, es esencial el establecimiento de objetivos en los distintos niveles de la entidad, ya que estos proporcionan el marco de referencia para identificar, analizar y gestionar los riesgos de manera alineada con las metas organizacionales.

La ISO 31000 señala que la evaluación de riesgos puede considerar criterios cualitativos y cuantitativos para describir, analizar y priorizar riesgos, lo que permite incluir las siguientes dimensiones:

- **Velocidad**: Tiempo que transcurre desde que el riesgo se activa hasta que genera impacto.
- **Volatilidad**: Variabilidad o cambios inesperados en la naturaleza, frecuencia o magnitud del riesgo.
- **Interdependencias**: Conexión con otros riesgos que pueden amplificar sus efectos (riesgos sistémicos o en cascada).
- **Persistencia**: Duración y sostenibilidad de los efectos una vez que el riesgo se ha materializado.
- **Impacto en el valor público**: Variable específica para el sector público. Se refiere al grado en que un riesgo puede afectar la creación, protección o sostenimiento del valor público que generan las instituciones estatales a través de sus políticas, programas y servicios.

La incorporación de estas variables dependerá del nivel de madurez del marco del proceso de gestión de riesgos adoptado por la institución.

En el **Anexo N° 1** se describen conceptos sobre dimensiones o criterios cualitativos adicionales en la evaluación de riesgos.

2. Conceptos Generales sobre Gestión de Riesgos

Como se señaló, las tendencias en materias de administración están dirigidas a la creación y mantenimiento de gobiernos corporativos fuertes que propendan a la transparencia en el quehacer de las entidades, a la responsabilidad y probidad de los integrantes del directorio y los administradores y a la creación de valor para los interesados o stakeholders**,** en este caso, para el ciudadano. Para lograr todo ello, la alta dirección cuenta con herramientas como la gestión de riesgos y el sistema control interno. La primera como un proceso para identificar, evaluar, tratar y controlar potenciales eventos o situaciones, con el fin de proporcionar un aseguramiento razonable respecto del logro de los objetivos de la organización; y el segundo, entendido como un sistema de acciones y medidas asumidas por quienes toman las decisiones para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidas.

En el ámbito de la gestión de riesgos, las organizaciones de todos los tipos y tamaños se enfrentan a factores internos y externos que hacen incierto saber si y cuándo van a alcanzar sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización, se denomina riesgo[2]. La Gestión de Riesgos es un proceso estructurado, consistente y continuo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos. Todos en la organización juegan un rol en el aseguramiento de éxito de la Gestión de Riesgos, pero la responsabilidad principal de la misma recae sobre la Dirección.[3]

La definición anterior se puede complementar con otros importantes elementos:

- La Gestión de Riesgos es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.
- Puede ser aplicada a todos los niveles de una organización, es decir, en los niveles estratégicos, tácticos y operacionales.
- También puede ser aplicada a proyectos específicos, para sustentar decisiones específicas o para administrar áreas específicas de riesgo.
- Para cada fase del Proceso de Gestión de Riesgos deberían mantenerse registros adecuados, suficientes como para satisfacer los requerimientos de una auditoría externa o certificación independiente.
- No sólo considera la identificación y tratamiento de riesgos, sino que también las oportunidades que contribuyan al logro de los objetivos.
- La aplicación del marco teórico del Proceso de Gestión de Riesgos siempre debe adecuarse a la entidad y al sector que ésta pertenece.

[2] NCh-ISO 31000:2018.
[3] Marco Gestión de Riesgos Empresariales COSO ERM.

3. Beneficios Potenciales de la Aplicación de la Gestión de Riesgos

- Mejora las posibilidades de alcanzar los objetivos en la organización.
- Incrementa el entendimiento de riesgos claves y sus implicaciones en la organización.
- Se identifica y comparte la responsabilidad de la administración de los riesgos del negocio.
- Genera y fortalece el enfoque en asuntos que realmente importan a la organización.
- Contribuye a disminuir las sorpresas y crisis en la organización.
- Incrementa la posibilidad de que cambios e iniciativas de proyectos puedan ser logrados en mejor forma.
- Mejora las capacidades de tomar mayor riesgo por mayores recompensas sociales y económicas.
- Genera más información y con más transparencia sobre los riesgos identificados, tomados y el fundamento de las decisiones realizadas.

La gestión de riesgos debe considerar al definir los criterios de riesgo, el "Apetito de Riesgo" de la organización gubernamental. Este concepto se ha definido en algunos marcos de control interno y de gestión de riesgos como: la cantidad de riesgo, desde un punto de vista amplio, que una organización está dispuesta o desea aceptar en la persecución de valor[4]; el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad[5] o la cantidad y tipo de riesgo que una organización desea retener o perseguir[6]. Esto es, cuánto riesgo se puede aceptar para dar cumplimiento a su misión institucional, objetivos estratégicos y entregar un servicio de calidad, agregando valor a los usuarios, beneficiarios o a la comunidad toda. El apetito de riesgo debe ser revisado por la dirección por lo menos una vez al año, junto con la estrategia de la organización y los procesos de planificación.

También hay que considerar el concepto de "Tolerancia al Riesgo", que son las variaciones aceptables con relación al logro de un objetivo de negocio específico, el que debe alinearse con el apetito del riesgo de una organización. Este considera cuánta variación puede aceptarse en el cumplimiento de los objetivos y la atención a los ciudadanos. Dicho de otra forma, la tolerancia al riesgo es la variación máxima de un riesgo que una organización gubernamental está dispuesta a aceptar para lograr sus objetivos.

Otro concepto importante que se debe considerar al definir los criterios es la "Capacidad de Riesgo", que hace referencia a la cantidad y tipo de riesgo máximo que una organización pública es capaz de asumir en la persecución de sus objetivos, dado sus recursos y capacidades.

Los conceptos antes señalados deben ser considerados al implementar el Proceso de Gestión de Riesgos, especialmente cuando las organizaciones gubernamentales formulen y presenten para su aprobación al CAIGG, un modelo adaptado a sus características y necesidades específicas. Lo anterior, teniendo en cuenta que hay organizaciones gubernamentales que tienen un apetito de riesgo mayor que otras para alcanzar sus objetivos (por ejemplo, las entidades de apoyo social potencialmente tienen mayor exposición al riesgo por el tipo de usuario vulnerable), así como cada una de estas tendrá niveles distintos de apetito y tolerancia al riesgo.

En **Anexo N° 2** se describen conceptos generales sobre apetito de riesgo y tolerancia al riesgo.

[4] Marco Gestión de Riesgos Empresariales COSO ERM.
[5] Marco Integrado de Control Interno – COSO I (Versión 2013).
[6] NCh-ISO GUIA 73:2012.

4. Componentes de la Norma NCH-ISO 31000:2018

Si bien existe una diversidad de marcos o *framework* internacionales para la gestión de riesgos, en principio su concepto global es el mismo, con fundamentos financieros, matemáticos o analíticos quizá distintos.

La Norma NCh-ISO 31000:2018 recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco cuyo objetivo es integrar el proceso de gestión de riesgos en general en la gobernanza de la organización, la estrategia y la planificación, la gestión, los procesos de información, las políticas, los valores y la cultura, de manera que sea un proceso integrado en toda la entidad.

La gestión de riesgos puede aplicarse a toda una organización, en sus áreas y niveles, en cualquier momento, así como a las funciones específicas, proyectos y actividades.

4.1 Principios de Gestión de Riesgos

Para que la gestión del riesgo sea eficaz y eficiente, y pueda crear y proteger el valor de la organización debería cumplir en todos sus niveles con los siguientes principios, de la **Figura N°1**:

Figura N° 1: Principios de Gestión de Riesgos

Fuente: NCh-ISO 31000:2018 – INN

- **Integrada**

La gestión del riesgo es parte integral de todas las actividades de la organización.

- **Estructurada e Integral**

Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

- **Adaptada**

El marco de referencia y el proceso de la gesti6n del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organizaci6n relacionados con sus objetivos.

- **Inclusiva**

La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.

- **Dinámica**

Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

- **Mejor Información Disponible**

Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en sus expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.

- **Factores Humanos y Culturales**

El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.

- **Mejora Continua**

La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

4.2 Marco de Referencia

El éxito de la gestión de riesgos dependerá de la efectividad del marco para manejar los riesgos, que provee las bases y fundamentos que traspasa la organización en todos sus niveles. El marco colabora en la gestión efectiva de los riesgos, a través de procesos de administración de riesgos en varios escenarios y contextos de la organización gubernamental. El marco asegura que la

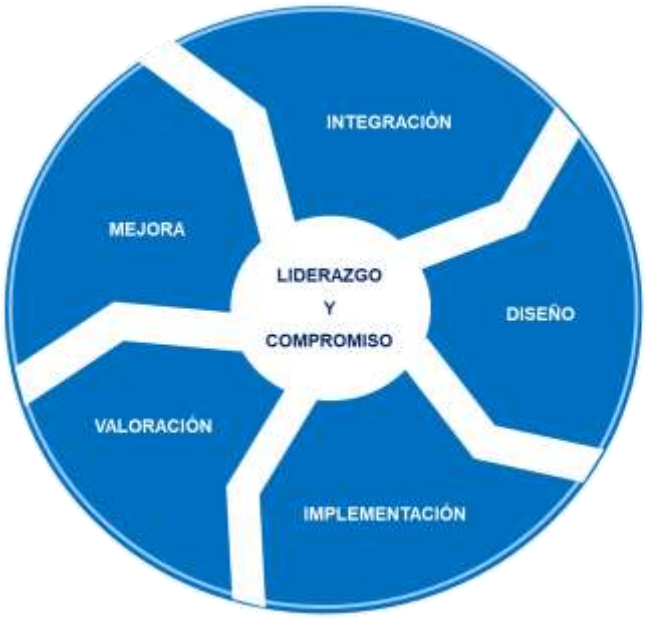
información derivada de ese proceso sea adecuadamente comunicada y se utilice como una base para la toma de decisiones por parte de la autoridad y para la rendición de cuentas o accountability de las mismas.

El marco de trabajo no pretende prescribir un sistema de gestión, sino más bien ayudar a la organización a integrar la gestión del riesgo en su sistema de gestión global. Por ello, las organizaciones deberían adaptar los componentes del marco de trabajo a sus necesidades específicas.

Si las prácticas y procesos de gestión existentes en una organización incluyen componentes de gestión del riesgo, o si la organización ya ha adoptado un proceso formal de gestión del riesgo para tipos o situaciones particulares de riesgo, entonces éstos se deberían revisar y evaluar de forma crítica de acuerdo con esta norma, a fin de determinar si la gestión de riesgos ha sido adecuada y eficaz.

El marco describe los elementos necesarios para la gestión de riesgos y la forma cómo estos componentes se interrelacionan entre sí, como se señala en la **Figura N°2** a continuación.

Figura N° 2: Marco de Referencia



Fuente: NCh-ISO 31000:2018 – INN

La descripción de los elementos del marco de trabajo de la gestión del riesgo comprende:

- **Liderazgo y Compromiso**

La introducción de la gestión del riesgo y el aseguramiento de su eficacia continua requieren un liderazgo y compromiso fuerte y sostenido por parte de la dirección de la organización, así como el establecimiento de una planificación estratégica rigurosa para lograr el compromiso a todos los niveles. La dirección y los órganos de supervisión deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización.

- **Integración**

Por su parte, la integración de la gestión del riesgo depende de la comprensión de las estructuras y el contexto de la organización. Las estructuras organizacionales difieren dependiendo del propósito, las metas y la complejidad de la entidad. El riesgo se gestiona en cada parte de la estructura de la organización y todos sus miembros tienen la responsabilidad de gestionar el riesgo.

- **Diseño del Marco de Referencia**

Comprensión de la organización y de su contexto. Antes de iniciar el diseño y la implementación del marco de trabajo de la gestión del riesgo, es importante evaluar y entender el contexto externo y el contexto interno de la organización, dado que ambos pueden influir significativamente en el diseño del marco de trabajo.

Articulación del compromiso con la gestión del riesgo: La dirección y los órganos de supervisión, cuando corresponda, deberían articular y demostrar su compromiso continuo con la gestión del riesgo mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de la entidad con la gestión del riesgo.

Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización: La dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurarse de que las autoridades, las responsabilidades y la obligación de rendir cuentas de los roles relevantes con respecto a la gestión del riesgo se asignen y comuniquen a todos los niveles de la organización.

Asignación de recursos: La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar la asignación de los recursos apropiados para la gestión del riesgo.

Establecimiento de la comunicación y la consulta: La entidad debería establecer un enfoque aprobado con relación a la comunicación y la consulta, para apoyar el marco de referencia y facilitar la aplicación eficaz de la gestión del riesgo.

- **Implementación**

La entidad debería implementar el marco de referencia de la gestión del riesgo mediante el desarrollo de un plan apropiado incluyendo responsables, plazos y recursos; la identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización; la

modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario; el aseguramiento de que las disposiciones de la organización para gestionar el riesgo son claramente comprendidas y puestas en práctica.

- **Valoración**

Para valorar la eficacia del marco de referencia de la gestión del riesgo, la entidad debería: medir periódicamente el desempeño del marco de referencia de la gestión del riesgo con relación a su propósito, sus planes para la implementación, sus indicadores y el comportamiento esperado; determinar si permanece idóneo para apoyar el logro de los objetivos de la entidad.

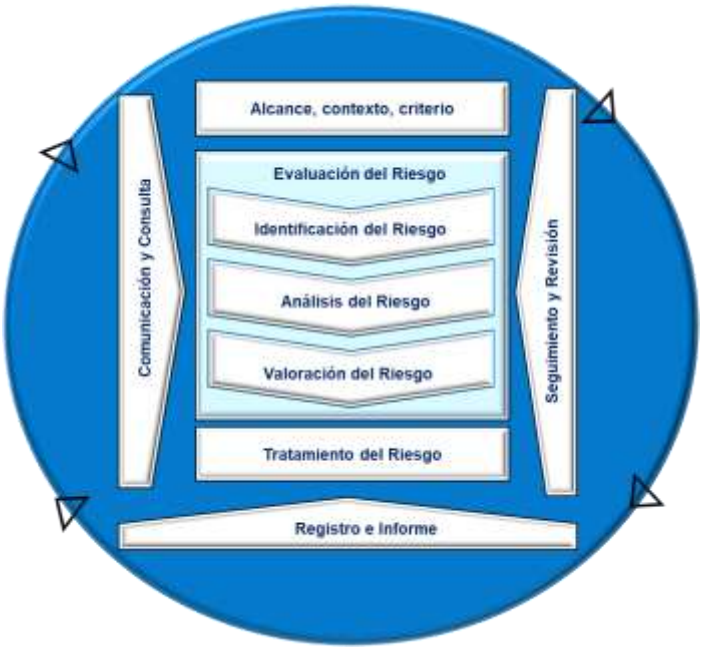
- **Mejora**

La entidad debe impulsar de manera continua la mejora de la idoneidad, adecuación y eficacia del marco de referencia para la gestión del riesgo, así como optimizar la integración del proceso de gestión de riesgos en todas sus actividades.

1.1 Proceso

Sin perjuicio que en la actualidad existen una serie de modelos para la gestión de riesgos de mayor o menor difusión, el CAIGG ha decidido utilizar un modelo genérico, que recoge en su mayor parte los elementos del Proceso de Gestión de Riesgos contenidos en la Norma NCh-ISO 31000:2018, que en su desarrollo y mejora a través del tiempo permita a las organizaciones gubernamentales adecuarlo a otros más específicos, si es que aquello fuese necesario.

Figura N° 3: Proceso de la Gestión de Riesgos



Fuente: NCh-ISO 31000:2018 – INN

- **Fases Genéricas del Proceso de Gestión de Riesgos**

Las fases en que se desagrega este modelo genérico y que deberán desarrollarse para implementar el Proceso de Gestión de Riesgos en organizaciones gubernamentales, se señalan a continuación:

Comunicación y Consulta: Los procesos continuos e iterativos que realiza una organización para proporcionar, compartir u obtener información y para comprometer el diálogo con las partes interesadas en relación con la gestión del riesgo. Comprende definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos. Dichos mecanismos deben permitir a las autoridades tomar decisiones en forma oportuna respecto de los riesgos con mayores desviaciones en relación con los niveles aceptados.

Establecimiento del Alcance, Contexto y Criterios: Definición de los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo, y se establecen el alcance y los criterios de riesgo para la política de gestión del riesgo. Comprende establecer los contextos estratégicos, organizacional y de gestión en los cuales tendrá lugar el Proceso de Gestión de Riesgos. Deben establecerse los objetivos de la evaluación del riesgo, los criterios contra los cuales se evaluarán los riesgos, el programa de evaluación del riesgo y definirse la estructura de análisis, los roles y responsabilidades.

Evaluación del Riesgo: La evaluación del riesgo es el proceso global de identificación del riesgo, de análisis del riesgo y de valoración del riesgo.

- **Identificación del Riesgo:** Tiene como objetivo la búsqueda, reconocimiento y descripción de riesgos que pueden ayudar o impedir a una entidad lograr sus objetivos. Comprende identificar los riesgos que podrían impedir, degradar o demorar el cumplimiento de los objetivos estratégicos y operativos de la organización, así como las oportunidades que puedan contribuir al logro de los referidos objetivos. También se deben identificar señales de alerta de delitos LA/FT/DF asociadas a los riesgos, cuando corresponda.

- **Análisis del Riesgo:** Tiene como objetivo contribuir a comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis del riesgo proporciona las bases para la valoración del riesgo y para tomar las decisiones relativas al tratamiento del riesgo. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. Consecuencia y probabilidad se combinan para producir un nivel estimado de riesgo según la definición de la organización. Adicionalmente se debe identificar y analizar los controles mitigantes existentes.

- **Valoración del Riesgo:** Tiene como objetivo contribuir a la toma de decisiones mediante la comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. Comprende comparar los niveles de riesgo encontrados contra los criterios de riesgo aceptado preestablecidos por la organización, considerando el balance entre beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

Tratamiento del Riesgo: Una vez completada la evaluación y valoración del riesgo, se debe realizar el tratamiento del riesgo. Este involucra la selección y el acuerdo para aplicar una o varias opciones pertinentes para cambiar la probabilidad de que los riesgos ocurran, los efectos de los riesgos, o ambas, y la implementación de estas opciones. A continuación de esto, sigue un proceso crítico de reevaluación del nuevo nivel de riesgo, con la intención de determinar su

tolerancia con respecto a los criterios previamente establecidos, para decidir si se requiere tratamiento adicional. De acuerdo con el ranking de riesgos y al nivel de riesgo aceptado preestablecido por la organización, definir su tratamiento y/o monitoreo, desarrollando e implementando estrategias y planes de acción específicos, que mantengan el riesgo dentro de los niveles aceptados por la organización.

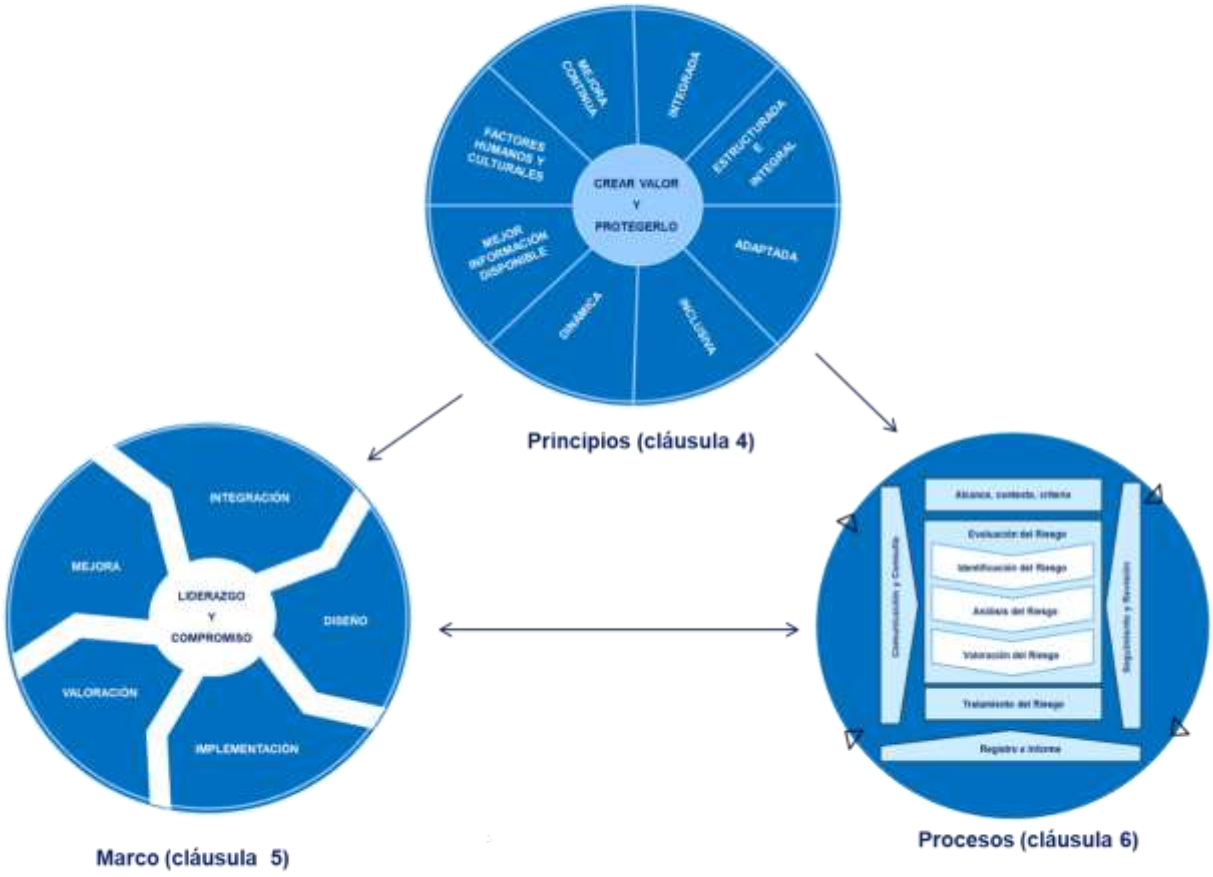
Seguimiento y Revisión: Como parte del proceso de gestión del riesgo, los riesgos y los controles se deben monitorear y revisar de manera regular. Comprende definir y utilizar mecanismos para la verificación, supervisión, observación crítica o determinación del estado de los riesgos y controles con objeto de identificar de una manera continua los cambios que se puedan producir en el nivel de desempeño requerido o esperado y dar cuenta de la evolución del nivel del riesgo en procesos críticos para la administración.

Registro e Informe: El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados a las autoridades con la finalidad de que cuenten con información oportuna y veraz para la toma de decisiones.

5. Relación entre los Componentes de la Norma NCh-ISO 31000:2018

Según lo descrito previamente, la Norma NCh- ISO 31000:2018 proporciona directrices para la gestión del riesgo que afectan a los objetivos de las entidades. Esta gestión del riesgo está basada en los principios, el marco de referencia y el proceso, de acuerdo con cómo se presenta en la **Figura N° 4**. Estos tres componentes interrelacionados podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos para que la gestión del riesgo sea eficiente, eficaz y coherente.

Figura N° 4: Relación entre Principios, Marco de Referencia y Proceso



Fuente: NCh-ISO 31000:2018 – INN

Si el lector requiere ahondar en la teoría que sustenta la Gestión de Riesgos Corporativos, puede acudir, entre otras, a las siguientes fuentes de información:

- Norma NCh-ISO 31000:2018 **-** Directrices para la Gestión de Riesgos. www.inn.cl.
- Norma ISO 31000:2018 Risk management - Guidelines. www.iso.org.
- Marco COSO ERM. www.erm.coso.org. y www.coso.org.
- Estándar Australiano/Neozelandés AS/NZS 4360:1999.
- OCEG, Red Book GRC Capability Model. www.oceg.org.

6. Relación con el Aseguramiento y la Auditoría Interna

A la Unidad de Auditoría Interna, le corresponderá entregar aseguramiento sobre el Proceso de Gestión de Riesgos que desarrolle la organización gubernamental, de acuerdo con las directrices establecidas por el CAIGG en esta materia y a los aspectos relevados en las Guías de Gestión y Servicios de Auditoría Interna (GGSAI) N°s 3, 4, 5, 6 y 7. Se contribuirá así, a la revisión permanente y mejora continua del proceso, que permita prevenir y mejorar aspectos del

funcionamiento del Proceso de Gestión de Riesgos como un todo. Cabe señalar que la retroalimentación específica, entregada en los Informes de Auditoría, que refiere a procesos en particular sometidos a evaluación durante el año, conforme al Plan Anual de Auditoría, también es parte del aseguramiento al Proceso de Gestión de Riesgos.

En este contexto, es necesario también, que los auditores internos entreguen aseguramiento razonable a sus Jefes de Servicio, acerca del nivel de cumplimiento de los planes de tratamiento de los riesgos identificados y presentados al CAIGG en forma periódica. De esta manera, el auditor interno entregará su opinión acerca del tratamiento de los riesgos críticos priorizados en la organización gubernamental y si los planes formulados han logrado mitigar los riesgos hasta un nivel aceptable para la misma o si por el contrario se requiere reformular dichas medidas.

IV. COMPONENTES ESTRUCTURALES DEL SISTEMA DE GESTIÓN DE RIESGOS

1. Marco de Trabajo Institucional para la Gestión de Riesgos

Desde el año 2014, las actividades incluidas en cada elemento del Marco de Trabajo de la Gestión del Riesgo han sido implementadas y actualizadas de manera progresiva, en alineación con el Proceso de Gestión de Riesgos. Este proceso se ha desarrollado en paralelo con la implantación de la gestión de riesgos, asegurando su integración en la estructura organizacional y operativa de las entidades públicas.

Inicialmente, la implementación se realizó con base en la Norma Chilena NCh-ISO 31000:2012, la cual establecía principios y directrices para la gestión de riesgos en distintos tipos de organizaciones. No obstante, a partir del año 2022, se adoptó la Norma NCh-ISO 31000:2018, que mantiene un enfoque actualizado y adaptable a cualquier organización, proporcionando un marco común que facilita la gestión de cualquier tipo de riesgo en el sector público, así como en otras industrias.

En este sentido, el proceso de gestión de riesgos de cada entidad pública debe estar sustentado en un marco de trabajo institucional que garantice su implementación, mantenimiento y mejora continua. Este marco debe considerar el liderazgo y compromiso de la alta dirección, la integración de la gestión de riesgos con los procesos institucionales, y la existencia de recursos, metodologías y estructuras claras que permitan operativizar el proceso. En coherencia con la norma ISO 31000:2018, el marco de trabajo debe contemplar: liderazgo, diseño, implementación, evaluación y mejora del sistema. Su propósito es asegurar que el proceso de gestión de riesgos se mantenga como una función transversal, dinámica y alineada con la estrategia institucional.

2. Gobernanza del Sistema de Gestión de Riesgos

La gobernanza del riesgo define los roles, responsabilidades y mecanismos de supervisión que permiten la conducción efectiva del proceso de gestión de riesgos. La autoridad máxima de la entidad es responsable de aprobar la política de gestión de riesgos y de asignar recursos para su desarrollo. Debe existir una instancia coordinadora, como un Comité de Riesgos, encargada de validar la identificación, evaluación y tratamiento de los riesgos críticos. Asimismo, las unidades técnicas y operativas tienen responsabilidades específicas en la identificación y tratamiento de los riesgos que les afectan directamente. La función de auditoría interna tiene un rol clave de aseguramiento independiente, contribuyendo a evaluar la eficacia del sistema. Toda esta estructura debe articularse con los lineamientos emitidos por el CAIGG.

3. Articulación con la Planificación Estratégica, Auditoría Interna y Control Interno

La gestión de riesgos constituye un componente estructural del sistema de gobernanza institucional y debe integrarse de manera sistémica a los procesos de planificación estratégica, control interno y aseguramiento independiente. En concordancia con los principios establecidos en la GGSAI N°3, los riesgos estratégicos deberán identificarse a partir del análisis de los objetivos institucionales, del contexto y del apetito de riesgo definido por la autoridad competente, transformándose en insumos clave para la toma de decisiones y la asignación de recursos.

El sistema de control interno deberá diseñarse y evaluarse sobre la base de una gestión de riesgos formal, documentada y dinámica, que permita anticipar desviaciones respecto del logro de los objetivos, fortaleciendo controles preventivos, detectivos y correctivos en función del nivel de exposición institucional.

Por su parte, la auditoría interna, en coherencia con el enfoque de aseguramiento basado en riesgos, deberá utilizar la información proveniente del proceso de gestión de riesgos para planificar sus trabajos con enfoque prioritario en las áreas de mayor criticidad, evaluando la eficacia del sistema de control interno y la adecuada gestión de los riesgos significativos.

Esta articulación entre planificación, gestión de riesgos, control interno y aseguramiento independiente fortalece la coherencia institucional, optimiza el uso de recursos y contribuye a la protección y generación de valor público.

4. Modelo de Madurez del Proceso de Gestión de Riesgos

Con el objeto de fortalecer un enfoque evolutivo, preventivo y de mejora continua del Sistema de Gestión de Riesgos, las organizaciones gubernamentales deberán evaluar anualmente el nivel de desarrollo y efectividad de su modelo de gestión, mediante la aplicación del Modelo de Madurez establecido en el presente Documento Técnico.

Este instrumento constituye un componente estructural del sistema, alineado con los principios de gobernanza, responsabilidad directiva y supervisión establecidos en las GGSAI, permitiendo medir el grado de integración del riesgo en la planificación estratégica, el control interno y la toma de decisiones institucionales.
La aplicación del modelo no tendrá un carácter meramente diagnóstico, sino que servirá como insumo formal para la asesoría que brinda el CAIGG, la definición de planes de fortalecimiento y la rendición de cuentas en materia de gestión de riesgos.

El detalle metodológico, niveles de madurez, criterios de evaluación y mecanismo de reporte anual se encuentran desarrollados en el **Anexo N° 3** del presente Documento Técnico, el cual forma parte integrante y obligatoria del Sistema de Gestión de Riesgos.

V. PROCESO DE GESTIÓN DE RIESGOS

El proceso de gestión de riesgos constituye el núcleo operativo del sistema, permitiendo a las entidades públicas identificar, analizar, valorar, tratar y monitorear los riesgos que pueden afectar el logro de sus objetivos estratégicos, operacionales, financieros, de cumplimiento e integridad.

Este capítulo establece las fases metodológicas del proceso de gestión de riesgos, conforme a los lineamientos de la NCh-ISO 31000:2018, el Marco COSO-ERM, las directrices del CAIGG, así como los criterios técnicos promovidos por las NOGAI (Normas Globales de Auditoría Interna), en aquellas materias que corresponda.

Cada fase descrita a continuación debe ser comprendida e implementada de manera integrada, secuencial y cíclica, respetando la naturaleza dinámica del riesgo y su permanente interacción con el entorno institucional.

El proceso es transversal, adaptable a todo tipo de unidades, funciones y niveles jerárquicos, y debe ser aplicado tanto en la implantación inicial del sistema como en su mantención y actualización periódica, de forma que apoye la toma de decisiones, la asignación eficiente de recursos y la generación de valor público.

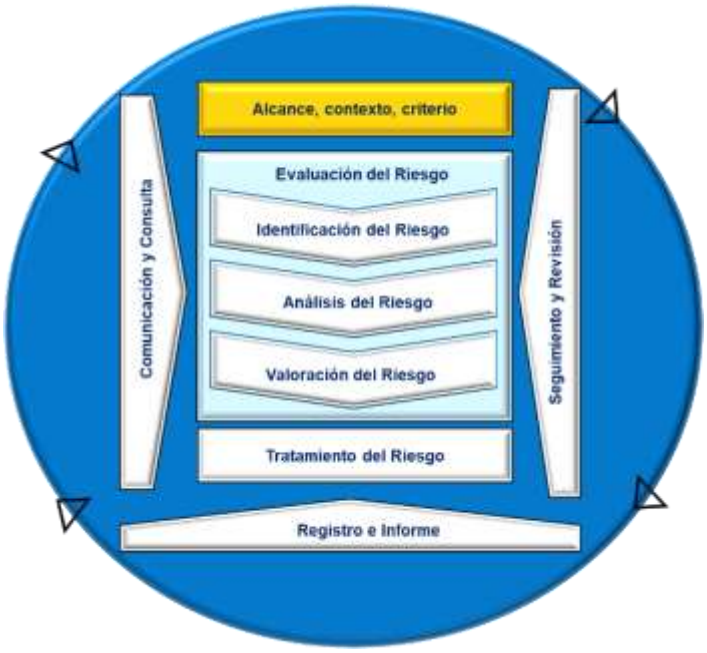
1. Fase: Establecimiento del Alcance, Contexto y Criterios

En esta fase fundamental del Proceso de Gestión de Riesgos, se establecen los elementos clave que permitirán definir el marco en el que se identificará, evaluará y tratará el riesgo dentro de la organización. En ella se determina:

- Qué se va a analizar (alcance).
- Qué factores influyen (contexto interno y externo).
- Cómo se evaluarán los riesgos (criterios).

Esta fase se presenta en la **Figura N° 5.**

Figura N° 5: Fase Alcance, Contextos, Criterios



Fuente: NCh-ISO 31000:2018 – INN

1.1 Alcance de la Gestión de Riesgo

En el contexto de la gestión de riesgos, el alcance se refiere a la definición clara de los límites, objetivos y enfoque del Proceso de Gestión de Riesgos. Este elemento es esencial para garantizar que el proceso sea efectivo y relevante, ya que establece qué áreas, actividades o aspectos de la organización estarán incluidos o excluidos en el análisis y tratamiento de los riesgos.

De acuerdo con el modelo metodológico adoptado por el CAIGG, el Proceso de Gestión de Riesgos debe aplicarse en un alcance a nivel de procesos, desagregados en subprocesos y etapas.

Dentro de la señalada desagregación en procesos, subprocesos y etapas, se incorporan conceptos como la clasificación en procesos transversales en la Administración del Estado, la tipificación de riesgos y la ponderación porcentual de la importancia estratégica de los subprocesos que componen los procesos en la organización, que también deben ser incorporados dentro del contexto de la gestión de riesgos.

a. Desagregación de Procesos Críticos

Para levantar información de los procesos, la técnica a utilizar para documentar y estructurar el trabajo corresponde a la desagregación de la información de procesos críticos de la institución en una Matriz de Riesgos Estratégica. Esta técnica permite correlacionar la estructura desagregada de un proceso (subprocesos y etapas) con los objetivos estratégicos y/u operativos.

En general, el Proceso de Gestión de Riesgos se inicia con los procesos críticos de la entidad, para ir ampliándose a una mayor cobertura, de manera de considerar todos los procesos que incidan en el logro de los objetivos de la organización gubernamental.

Esta técnica tiene las siguientes ventajas:

- Obliga al personal encargado a conocer e interactuar en forma integral con su organización.
- Permite construir la Matriz de Riesgos de la organización gubernamental de tipo global y las matrices específicas para cada proceso relevante o materia específica que se requiera analizar.
- Se genera una sólida base para aplicar y documentar el Proceso de Gestión de Riesgos.

b. Identificación y Priorización de Procesos Críticos en la Institución (Paso N° 1 en la Matriz de Riesgos)

Para efectos de este documento, se entenderá como proceso un conjunto de actividades íntimamente relacionadas que existen para generar un bien o un servicio, que cuentan con un ingreso de recursos, una transformación de éstos y una salida de servicios o productos, que tienen un cliente interno o externo a la organización. Podemos agregar a esta definición, que aquellos identificados como claves para el logro de la misión institucional a través del cumplimiento de los objetivos estratégicos, serán los procesos críticos.

Es necesario reiterar que la identificación de procesos, subprocesos y etapas es una labor que las organizaciones gubernamentales deberían tener realizada y respaldada a través de documentos formales, tales como; bases técnicas, términos de referencia, reglamentos y normativas internas de los programas y servicios que entregan las instituciones.

En caso de que dichas estructuras estén implícitas en la documentación o no estén formalizadas, se debe analizar e identificar en conjunto con los ejecutivos y directivos responsables, la estructura de los procesos. Con esa información se debe analizar la relación entre la misión objetivos estratégicos formales declarados y los procesos organizacionales, identificando para cada proceso específico, el nivel de contribución que realiza a cada objetivo estratégico, mediante la metodología definida por el CAIGG.

Tal como se señaló, hay que tener presente que muchos procesos inciden en forma indirecta en el logro de los objetivos, ya que constituyen soporte para la realización de diversas acciones de negocio, otros en cambio, inciden en forma directa. Debido a estas particularidades en la organización, se ha estimado necesario formular un método que permita distinguir entre el nivel de contribución o relevancia de cada uno de los procesos.

El nivel de contribución que realiza un determinado proceso al cumplimiento de los objetivos estratégicos de la organización gubernamental ya sea un proceso relevante que desarrolla esta organización tanto a nivel estratégico externo, con el objetivo de satisfacer a sus usuarios; como a nivel interno, con la finalidad de definir el soporte administrativo de la labor de la Institución, se medirá de acuerdo con los criterios del **Cuadro N° 1**:

Cuadro Nº 1: Escala para Medir el Nivel de Contribución que Afecta el Cumplimiento del Objetivo Estratégico

Clasificación del Nivel	Descripción del Nivel de Contribución	Valor
Alto	El proceso aporta de manera fundamental en el cumplimiento del objetivo estratégico.	3
Medio	El proceso aporta de manera importante en el cumplimiento del objetivo estratégico.	2
Bajo	El proceso aporta de manera menor en el cumplimiento del objetivo estratégico.	1
Nulo	El proceso no aporta en el cumplimiento del objetivo estratégico.	0

A continuación, se presenta un esquema matricial que permite identificar los procesos críticos de acuerdo con esta metodología, al relacionar cada uno de los procesos de la organización gubernamental con los objetivos estratégicos de la misma. El procedimiento específico corresponderá al siguiente:

Una vez identificados todos los procesos que existen en la organización, se debe aplicar la siguiente metodología para determinar la priorización de los procesos en base a su nivel de contribución para todos los objetivos estratégicos. Análisis que posteriormente servirá para determinar cuáles serán los procesos críticos que se les realizará el modelamiento de riesgos, de acuerdo con el esquema del **Cuadro N° 2**.

Cuadro Nº 2: Esquema de Relación y Priorización de Procesos Relevantes en la Institución en relación con los Objetivos Estratégicos

Misión Institucional: xxxxxxx						
Objetivos / Procesos institucionales	**Objetivo Estratégico 1**	**Objetivo Estratégico 2**	**Objetivo Estratégico ...**	**Objetivo Estratégico n**	**Nivel de Contribución Promedio del Proceso al Cumplimiento de los Objetivos**	**Proceso seleccionado (2,0 – 3,0)**
Proceso 1	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Promedio Aritmético Proceso 1	X
	Justificación	Justificación	Justificación	Justificación		
Proceso 2	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Promedio Aritmético Proceso 2	X
	Justificación	Justificación	Justificación	Justificación		
Proceso 3	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Promedio Aritmético Proceso 3	-
	Justificación	Justificación	Justificación	Justificación		
……	.....	.....	.....	.....	.....	-
Proceso n	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Alto (3), Medio (2), Bajo (1), Nulo (0)	Promedio aritmético Proceso n	X
	Justificación	Justificación	Justificación	Justificación		

En el esquema presentado, se consideran todos los procesos organizacionales y los objetivos estratégicos de la organización gubernamental. Cada proceso se analiza en función de su contribución al cumplimiento de los objetivos estratégicos, clasificándolo en niveles Alto, Medio, Bajo o Nulo, según la escala previamente establecida. Este análisis debe incluir una justificación detallada para cada nivel asignado.

Finalmente, cuando se han relacionado todos los procesos con todos los objetivos estratégicos, se calcula el promedio entre los niveles de contribución individual entre procesos y objetivos, obteniéndose el nivel promedio por cada proceso. Por consiguiente, se contará con la información necesaria para determinar si se seleccionará el proceso para el análisis y modelamiento de riesgos.

La selección final de los procesos críticos se basará en la misma escala utilizada para medir el nivel de contribución y cumplimiento de los objetivos estratégicos. Para el análisis, se elegirán aquellos procesos cuya contribución promedio esté entre 2.0 y 3.0 puntos, lo que corresponde a un nivel de influencia importante o fundamental en el cumplimiento de los objetivos estratégicos institucionales.

En el **Cuadro N° 3** se detalla un ejemplo.

Cuadro Nº 3: Ejemplo: Selección de procesos críticos en una organización que cuenta con tres objetivos estratégicos

Misión Institucional: Proteger y mejorar la salud de la población mediante la prestación sanitaria, la regulación, fiscalización y provisión oportuna de prestaciones de salud con estándares de calidad, equidad y probidad					
Objetivos / **Procesos Institucionales**	Fortalecer el acceso oportuno y equitativo a prestaciones de salud en la red pública	Garantizar la calidad, seguridad y continuidad de la atención sanitaria.	Optimizar el uso eficiente y transparente de los recursos públicos del sector salud	**Nivel de contribución promedio del proceso al cumplimiento de los objetivos**	**Proceso seleccionado (2,0 – 3,0)**
Gestión de Redes Asistenciales	3	3	2	2,67	X
Justificación	La Gestión de Redes Asistenciales es estructural para el acceso oportuno y equitativo, ya que: • Define la organización territorial de la red. • Coordina derivaciones entre niveles de atención. • Determina priorización de listas de espera. • Administra capacidades hospitalarias y APS. Sin una gestión adecuada de redes, el objetivo estratégico 1 no puede cumplirse, pues la oportunidad y equidad dependen directamente del diseño y coordinación del sistema asistencial.	Este proceso incide directamente en la calidad y continuidad de atención mediante: • Protocolos de referencia y contrarreferencia • Coordinación de alta hospitalaria. • Gestión de continuidad clínica. • Integración entre atención primaria y hospitalaria. Errores en este proceso generan quiebres de continuidad, eventos adversos y deterioro en la seguridad del paciente.	La eficiencia del gasto sanitario depende parcialmente de la adecuada gestión de redes: • Evita duplicidades de prestaciones. • Reduce hospitalizaciones innecesarias. • Optimiza uso de camas críticas. • Disminuye traslados ineficientes. Si bien incide en eficiencia, no es el único proceso determinante del uso financiero.		El proceso tiene un promedio de 2,67, lo que lo posiciona como proceso crítico estratégico. Debe ser modelado obligatoriamente en la matriz de riesgos estratégica
Gestión de Comunicaciones Institucionales	1	1	1	1,0	No

Justificación	La comunicación puede apoyar campañas informativas sobre acceso, pero: • No define asignación de recursos. • No organiza la red asistencial. • No interviene en la gestión clínica. Su impacto es indirecto y de apoyo.	Puede difundir protocolos o campañas de seguridad, pero: • No gestiona procesos clínicos. • No controla estándares técnicos. • No define lineamientos asistenciales. Influye marginalmente.	Puede comunicar transparencia, pero: • No administra presupuesto. • No ejecuta gasto. • No controla eficiencia financiera. Su incidencia es secundaria.		Con un promedio de 1,0, no cumple el umbral (2,0–3,0). No se considera proceso crítico para efectos de modelamiento estratégico de riesgos. Podría evaluarse únicamente en matriz operativa si existieran riesgos reputacionales significativos.

Adicionalmente, podrán incluirse como procesos críticos aquellos que, aun cuando no alcancen el umbral promedio de contribución señalado, se encuentren expuestos a riesgos emergentes que puedan afectar significativamente la continuidad operativa, la sostenibilidad institucional, el cumplimiento normativo o la confianza pública.

Para estos efectos, se entenderá por riesgos emergentes aquellos eventos o condiciones nuevas, dinámicas o en evolución, cuya probabilidad o impacto pueden incrementarse debido a cambios normativos, tecnológicos, económicos, sociales, ambientales o institucionales, y que no necesariamente se reflejan en el análisis histórico de desempeño.

La identificación de riesgos emergentes deberá basarse en análisis prospectivo, revisión de tendencias, alertas de organismos rectores, cambios regulatorios, transformaciones digitales, nuevos modelos de prestación de servicios, u otros factores contextuales relevantes.

La inclusión de estos procesos deberá ser debidamente fundada y documentada por la autoridad competente o el comité de riesgos, incorporando una justificación técnica que evidencie su criticidad potencial y la necesidad de anticipar su modelamiento dentro del sistema de gestión de riesgos.

- **Universo de Procesos del Servicio**

El universo de procesos del servicio corresponde al conjunto total y exhaustivo de procesos estratégicos, misionales, de apoyo y transversales que conforman el quehacer institucional y permiten el cumplimiento de su mandato legal y de sus objetivos estratégicos.

La determinación del universo de procesos constituye una etapa previa e indispensable para la priorización y modelamiento de riesgos, ya que asegura que el análisis no se limite a procesos tradicionalmente visibles o históricamente auditados, sino que abarque de manera integral todas las actividades relevantes del servicio.

La identificación y formalización del universo de procesos del servicio no constituye un ejercicio meramente descriptivo, sino una condición estructural para una gestión de riesgos estratégica, integral y alineada con los estándares del sistema de control interno.

Sin un universo claramente definido, la priorización de procesos críticos carece de base metodológica sólida y puede derivar en omisiones significativas que afecten la calidad del modelamiento de riesgos institucionales.

c. Procesos Transversales en la Administración del Estado (Paso N° 2 en la Matriz de Riesgos)

Los procesos transversales son procesos definidos a nivel global de acuerdo con sus objetivos y productos finales. Dentro de ellos se agrupan los procesos específicos informados por las organizaciones gubernamentales con distintas denominaciones, pero que responden a una misma raíz.

Para garantizar una adecuada estructuración de la Matriz de Riesgos, las organizaciones gubernamentales deben clasificar sus procesos dentro de las categorías de procesos transversales. Esta clasificación permite estructurar el análisis de riesgos de manera homogénea y alineada con las mejores prácticas de gestión en la administración pública.

A continuación, se presenta el **Cuadro Nº 4**, que detalla las principales categorías de procesos transversales:

Cuadro Nº 4: Clasificación y Descripción de Procesos Transversales en la Administración del Estado

Procesos Transversales en la Administración del Estado	Descripción
Procesos de Negocios	
Subsidios a privados de fomento	Se entienden aquellos cuyo objetivo es promover, mediante incentivos económicos, que los particulares realicen por sí mismos actividades productivas.
Subsidios a privados social	Se entienden como tales los procesos cuyo objetivo es la promoción de ciertos objetivos sociales como la integración, etc.
Subsidios a privados asistencial	Consisten en procesos cuya finalidad es entregar ayuda de subsistencia a particulares.
Transferencias a/de otras entidades públicas	Son procesos en que, por ley o convenios, se entregan o reciben recursos de otro organismo del Estado.
Servicios de atención al ciudadano – contraprestación	Procesos que se orienten a servir a todos los ciudadanos a través de la entrega de atención, servicios o productos.
Servicios de atención social/ previsional /salud	Procesos que se orienten a prestar una atención de salud, previsional o social a personas que tengan ciertas calidades (Ej.: pensionados públicos, ancianos, personas de las fuerzas armadas, etc.)
Créditos - recuperación prestamos	Se refiere a procesos de entrega de préstamos, incluyéndose los procesos de planificación, ejecución y cobranzas.
Almacenamiento y distribución	Procesos que consistan en bodegaje, mantenimiento de stock y distribución de materiales o bienes.

Procesos Transversales en la Administración del Estado	Descripción
Infraestructura	Procesos que se refieran a los bienes muebles e inmuebles de la organización gubernamental que se utilizan para cumplimiento del rol de la misma.
Asesoría a infraestructura	Procesos que impliquen estudios y acciones que apoyen decisiones sobre la infraestructura.
Estudios para marco cultural	Procesos de estudios culturales que releven las artes, literatura, pintura y todo lo relacionado a temas culturales.
Estudios para regulaciones, normativa y fijación tarifaria	Procesos de estudios que sirvan o puedan servir de base para la emisión de normativa, regulaciones, tarifas, etc.
Administración de bienes estratégicos	Proceso a través del cual la organización gestiona aquellos bienes que son indispensables para el cumplimiento de su función; que son de la esencia de su "negocio".
Otorgamiento y/o reconocimiento de derechos	En el caso de aquellas organizaciones que entregan derechos o beneficios a personas naturales como ser parte de un registro, derechos de aguas, etc.
Estudios e investigaciones	Aquellos estudios cuyo sentido es investigar un tema económico, financiero, de mercado u otra situación determinada importante para la organización.
Legal estratégico	Desarrollo de acciones legales y/o judiciales como negocio de la organización gubernamental.
Control de outsourcing	Equivalen a la gestión y monitoreo de los contratos que externalizan funciones propias de la organización gubernamental.
Seguridad y Control de Personas y/o Recintos	Proceso relacionado con seguridad que realizan determinados entes del estado en relación con las personas en distintas calidades: victimas, imputados, reos, reclutas y la ciudadanía en general. Esto podría incluir operaciones de distinta naturaleza como vigilancia, traslados, control u otros de índole distinta, relacionados con la seguridad.
Seguridad del transporte	Procesos relacionados con seguridad operacional y respuestas ante situaciones de emergencias de los servicios de transporte terrestre, marítimo y aéreo, así como de las instalaciones portuarias y aeroportuarias o de cualquier otra índole, en donde exista tráfico de pasajeros o carga.
Calificación ambiental	Procesos relacionados a análisis, autorizaciones y permisos medio ambientales.
Producción de bienes materiales	Corresponde a aquellos procesos productivos que generan bienes materiales como resultado
Comercialización	Procesos que desarrollan aquellas organizaciones gubernamentales que venden productos y/o servicios a terceros.
Coordinación de Acciones de Emergencia	Procesos asociados a la ejecución y coordinación de operaciones de emergencia, gestión de recursos para emergencias, monitoreo y análisis de los diversos factores y elementos relacionados con situaciones de emergencia o catástrofes.
Procesos Gerenciales o de Dirección Estratégica	
Planificación presupuestaria	Proceso anual que se realiza en la organización para programar la presupuestación de las diversas acciones que ejecuta.
Planificación estratégica	Proceso que realiza la organización gubernamental en el que fija sus objetivos, sus metas y la forma como las cumplirá.

Procesos Transversales en la Administración del Estado	Descripción
Coordinación entre instancias	Procesos que implican relaciones entre diversos niveles, personas o entidades cuya organización y canalización son de responsabilidad de la organización gubernamental.
Gobierno de TI - Gobierno Electrónico	Procesos integrales para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar eficiencia y eficacia de la gestión pública e incrementar la transparencia del sector público y la participación de los ciudadanos a través del uso de las tecnologías de información y comunicaciones (TIC).
Conducta Ética y Valores Organizacionales	Procesos o mecanismos para definir, promover y reforzar la conducta ética y los principios éticos organizacional en todos los niveles de la Administración del Estado.
Transparencia	Procesos o mecanismos de transparencia activa y pasiva en la Administración del Estado.
Probidad/Anticorrupción	Procesos o mecanismos para controlar y vigilar los programas de probidad, integridad y/o anticorrupción en la Administración del Estado.
Cultura organizacional	Procesos o mecanismos para gestionar, controlar o vigilar las percepciones, sentimientos, actitudes, hábitos, creencias, valores, tradiciones y formas de interacción dentro y entre los grupos existentes en la organización.
Gestión del desempeño y rendición de cuentas (accountability)	Procesos o mecanismos para dirigir, gestionar y controlar la rendición de cuentas de las autoridades de la entidad pública.
Monitoreo y vigilancia del control y la gestión de riesgos	Procesos o mecanismos para monitorear y vigilar los resultados de los procesos de control y de gestión de riesgos en la entidad pública.
Comunicación de riesgos y controles a las áreas adecuadas	Procesos o mecanismos para gestionar, controlar y retroalimentar la comunicación de riesgos y controles a las áreas adecuadas dentro de la entidad pública.
Estructura organizacional de los órganos de gobernanza	Procesos o mecanismos para diseñar, implementar y controlar las estructuras organizacionales y su funcionamiento en la entidad pública.
Roles y responsabilidades organizacionales	Procesos o mecanismos para definir, implementar y controlar los roles y responsabilidades en la entidad pública.
Mecanismos de Incentivo de Remuneraciones.	Proceso a través del cual la organización controla el cumplimiento de las metas, indicadores, convenios de desempeño y otros similares. PMG, MEI, CDC, CDI y otras leyes relacionadas.
Proceso Gestión de Riesgos	Proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto del alcance de los objetivos de la organización, utilizando el Marco ISO NCh 31000 o uno equivalente.
Procesos de Inversión	
Iniciativas de inversión	Todos los procesos de inversión considerados en el subtítulo 31, desde los estudios a la ejecución.
Mercado financiero	Inversión en instrumentos financieros y de mercado accionario que realizan algunas organizaciones gubernamentales autorizadas.

Procesos Transversales en la Administración del Estado	Descripción
Procesos de Información	
Sistemas de información administrativos	Aquellos sistemas de información que entregan reportes y datos a los que puedan tener accesos terceros.
Sistemas informáticos	Soporte informático interno de la organización gubernamental, que comprende sistemas de información contable, financieros y operativos que contienen datos internos de dicha organización.
Procesos de Control Operativo de los Recursos Públicos	
Fiscalización	Procesos a través de los cuales las organizaciones gubernamentales controlan a entes externos en el cumplimiento de normas y estándares.
Evaluación y control de substancias	Proceso de control de substancias peligrosas.
Control de gestión	Proceso a través del cual la organización controla el cumplimiento de las metas, logros e indicadores que se ha definido en su planificación.
Control Interno Integral	Políticas, procedimientos (manuales y automáticos) y actividades, que forman parte de un enfoque de control, diseñados y operados para asegurar que los riesgos estén contenidos dentro de las tolerancias establecidas por el proceso de evaluación de riesgos, utilizando el Marco COSO I – 2013.
Procesos de Soporte	
Financiero	Procesos contables, de tesorería, registro presupuestario, etc.
Legal	Asesoría y apoyo jurídico dirigido al quehacer interno de la organización gubernamental.
Comunicaciones	Acciones de difusión y publicidad de los programas y acciones desarrolladas por la organización gubernamental.
Adquisiciones y abastecimiento	Incluye la programación de compra, licitación, compra, recepción y distribución de los bienes y servicios adquiridos.
Recursos humanos	Incluye todos los procesos relacionados al personal, su capacitación, remuneraciones, feriados y bienestar.
Administración/ mantenimiento recursos	Procesos de gestión de los recursos materiales de la organización gubernamental, inventario, baja y traslado.
Gestión documental	Procesos de administración, dirección, manejo, registro, archivo y almacenamiento de documentación de la organización gubernamental, con o sin apoyo de sistemas informáticos, referido tanto a documentación interna como externa de dicha organización.
Auditoría Interna	Proceso independiente y objetivo de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Se orienta a la prevención y contempla actividades de planificación, programación, ejecución, informe y seguimiento.
Recursos materiales	Incluye todos los procesos relacionados a los bienes muebles o raíces que utiliza la organización gubernamental para cumplimiento de sus objetivos.

Es necesario relevar que las organizaciones gubernamentales deben clasificar sus procesos solo en una de las categorías antes definidas, basados en las características organizacionales y en los objetivos de estos. Cuando existan dudas o diferencias respecto de la clasificación de uno o más procesos dentro de la categoría de procesos transversales, deberá consultarse y discutirse con el respectivo asesor del CAIGG, para la creación de un nuevo proceso transversal, si fuese necesario.

En el **Cuadro N° 5** se entrega un ejemplo de dicha clasificación.

Cuadro Nº 5: Ejemplo de Clasificación de Procesos Críticos

Proceso Transversal	Proceso	Subproceso	Etapas	Objetivos	----
Créditos – recuperación de préstamos	Entrega de créditos de fomento	Subproceso 1	Etapa 1	….	….
		Subproceso 2	….	….	….
Subsídios a privados de fomento	Programa de beneficios económicos para mujeres emprendedoras	….	….	….	….
Subsidios a privados social	Subsidios para capacitación	….	….	….	….
Subsidios a privados de fomento	Entrega de bonos para producción de leche	….	….	….	….
Recursos Humanos	Personal	….	….	….	….
Coordinación de Acciones de Emergencia	Proceso de alerta temprana	….	….	….	….
Adquisiciones y abastecimiento	Compras y contrataciones	….	….	….	….

Es importante tener en cuenta que la clasificación de los procesos en procesos de soporte, gerenciales, de negocio, entre otros, tiene un carácter genérico y referencial. Esta categorización no debe considerarse rígida ni universal, ya que la naturaleza de los procesos puede variar según el tipo de organización gubernamental y su misión institucional.

d. Identificación de Subprocesos en los Procesos Críticos (Paso N° 3 en la Matriz de Riesgos)

Una vez seleccionados los procesos críticos, de acuerdo con la metodología descrita, se deben identificar los subprocesos que integran cada uno de ellos (dependerá de la estructura del proceso y de las características organizacionales de la organización gubernamental). Los subprocesos corresponden a aquellos componentes principales en el desarrollo de los procesos.

Al igual que los procesos, los subprocesos que los componen pueden ser de diversa importancia y tener distinta influencia en la generación de los productos o servicios.

e. Ponderación Estratégica por Subprocesos Componentes de Procesos Críticos (Paso N° 4 en la Matriz de Riesgos)

Considerando que no todos los subprocesos tienen la misma importancia estratégica dentro de un proceso crítico, debe definirse por la dirección el peso relativo que cada subproceso tiene dentro de un proceso crítico, esto atendiendo a la relevancia o importancia estratégica que tiene cada subproceso en la consecución exitosa de los objetivos de cada proceso crítico. Esta

ponderación de los subprocesos debe ser justificada adecuadamente, considerándose para esta labor algunas variables como las siguientes:

- El impacto de la concreción de los riesgos en el subproceso para el proceso y la organización gubernamental.
- El grado de complejidad de las etapas que se identifican al interior del subproceso.
- Especialización del personal que se requiere para desarrollar las diversas etapas y actividades del subproceso.
- Los recursos involucrados y su cobertura regional.
- El uso de sistemas de medios de información, entre otros.
- Eficiencia de los sistemas de información del subproceso.
- Competencia, aptitud e integridad del personal.
- Nivel de sistemas computarizados de información.
- Oportunidad y efectividad de los sistemas de control interno.
- Cambios organizacionales, operacionales, tecnológicos y económicos.
- Características de los usuarios, clientes y proveedores.
- Complejidad y volatilidad de las actividades desarrolladas en el subproceso.
- Cambios organizacionales, operacionales, tecnológicos y económicos producidos.

La ponderación porcentual distribuida en todos los subprocesos componentes de un proceso crítico, debe sumar 100%.

Cuando existan dudas o diferencias que surjan respecto de la ponderación estratégica de los subprocesos, deberá consultarse y discutirse con el CAIGG.

A continuación, en el **Cuadro Nº 6** se entrega, a modo de ejemplo, la ponderación de subprocesos componentes de un proceso crítico de una organización ficticia, con la justificación correspondiente:

Cuadro Nº 6: Ejemplo de Justificación de la Ponderación Estratégica de Subprocesos componentes de un Proceso Crítico

Proceso	Descripción	Subprocesos	Pond.[7]	Justificación de la ponderación
Crédito de fomento para mujeres microempresarias	Se trata del proceso principal de la organización gubernamental, que cumple el objetivo estratégico de entregar apoyo a las iniciativas de la mujer microempresaria, involucra sobre M$ 20.000, y se orienta a usuarias en situación vulnerable, con ingresos anuales inferiores a las 200 UF. Además, es un instrumento para colaborar con la recuperación de las mujeres microempresarias afectadas por el terremoto	Postulación crédito	10%	La ponderación baja considera que la postulación es una acción externa, propia de las usuarias.
		Evaluación crédito	30%	Este subproceso es importante para el éxito del proceso por cuanto las deficiencias en la evaluación del crédito afectan la recuperación del mismo y la imagen de la organización gubernamental, por otra parte se trata de una labor altamente especializada, para la cual no siempre se cuenta con personal idóneo. Una mala evaluación puede dejar sin crédito a una mujer que perdió su negocio en el sismo.
		Entrega crédito	25%	Su nivel de complejidad es medio, pero se le pondera con este porcentaje puesto que una mala entrega podría afectar a otros usuarios beneficiarios de los incentivos.

[7] Porcentaje de Ponderación Estratégica de los subprocesos en relación con los objetivos del proceso.

Proceso	Descripción	Subprocesos	Pond.[7]	Justificación de la ponderación
		Recuperación crédito	35%	La baja recuperación repercute en el presupuesto de la organización gubernamental, afectando directamente a las otras usuarias y la imagen de la organización, además en la actualidad se hace manualmente y los errores en su registro son frecuentes.
Capacitación para los negocios	Se trata de un proceso importante, ya que colabora al cumplimiento del objetivo estratégico de entregar apoyo a las iniciativas de la mujer microempresaria, involucra un presupuesto superior a M$ 3.000 y se dirige a mujeres en situación vulnerable con baja escolaridad	Postulación	20%	Se trata de un beneficio conocido por la población objetivo, del cual se realiza difusión desde hace seis años con buena respuesta de las usuarias. El personal tiene experiencia y se cuenta con un sistema de información para el ingreso y validación de datos de los postulantes.
		Capacitación	50%	Se trata de cursos contratados en el mercado, entregados por personal externo a la organización, que debe ser monitoreado a fin de que entregue materias requeridas por las usuarias, con un nivel comprensible para el público objetivo, con la flexibilidad necesaria para mujeres y no siempre se cuenta con personal adecuado y recursos para la supervisión.
		Evaluación	30%	Es importante ya que es la forma de medir como se ha recibido por las usuarias los contenidos de los cursos y evaluar los resultados de los cursos. No se cuenta con personal idóneo en todas las materias para hacer la evaluación del curso y una mala capacitación afecta la imagen de la organización gubernamental.
Presupuesto y Contabilidad	Se trata de un proceso de soporte, que colabora a la ejecución de los procesos que genera los productos estratégicos de la organización gubernamental	Planificación	40%	Su importancia se debe a la complejidad de realizar una planificación adecuada con antecedentes efectivos de los recursos que se utilizarán en el año.
		Pagos	30%	Un pago mal realizado afecta la planificación y el registro, sin embargo, la adecuada planificación facilita el control de los pagos.
		Registro	30%	…..

f. Identificación de Etapas en cada Subproceso (paso N° 5 en la Matriz de Riesgos)

Cuando sea posible seguir desagregando la estructura para análisis dentro de cada subproceso (dependerá de las características y estructura del proceso y de la organización, entre otras variables), se deberá identificar las etapas que lo conforman y que equivalen a las acciones o actividades que en conjunto forman el subproceso.

Hay que destacar que existen casos en que la estructura de desagregación máxima posible será el subproceso y en otros será posible desagregar hasta el nivel de etapa que componen los subprocesos. Esta variable de análisis también dependerá de la naturaleza y estructura de cada organización gubernamental.

Una vez definido el último nivel de desagregación de cada proceso, se procederá a identificar los objetivos operativos.

g. Identificación de Objetivos Operativos (paso N° 6 en la Matriz de Riesgos)

Se entenderá por objetivos operativos, aquella meta o finalidad que se persigue cumplir mediante la ejecución de una etapa o mediante la ejecución de un subproceso; si la desagregación fue solo a nivel de subproceso. Siempre hay que tener presente que los objetivos del proceso, subproceso o etapa están establecidas a través de documentos formales (bases administrativas o técnicas, normas internas, programas, términos de referencia, etc.) en forma explícita o implícita, lo que implica una labor de estudio y análisis de la documentación regulatoria y de soporte en los procesos.

En el **Anexo Nº 4** se describen los pasos metodológicos para la formulación y validación de objetivos, complementando lo ya definido en la planificación estratégica institucional y en el levantamiento formal de procesos del servicio. Este anexo tiene por finalidad asegurar que los objetivos considerados en el proceso de gestión de riesgos cuenten con claridad conceptual, coherencia estratégica y trazabilidad respecto del mandato institucional.

Por su parte, el **Anexo Nº 5** contiene una guía metodológica para el levantamiento sistemático de información de los procesos institucionales, detallando los elementos mínimos que deben identificarse y documentarse, tales como propósito del proceso, responsables, entradas, actividades críticas, salidas, puntos de control, interacciones y riesgos asociados.

Ambos anexos constituyen instrumentos de apoyo técnico obligatorios para asegurar consistencia metodológica en la identificación, análisis y modelamiento de riesgos a nivel institucional.

1.2. Contexto Interno, Externo y de Gestión de Riesgos

Para establecer el contexto organizacional o interno, es necesario comprender y conocer, entre otros, la estructura interna, recursos humanos, filosofía y valores, políticas, misión, metas, objetivos y estrategias para lograrlos.

Para establecer el contexto estratégico o externo, es necesario analizar el entorno en que opera la organización, considerando aspectos tales como los financieros, operacionales, competitivos, políticos, de imagen, sociales, culturales, legales, clientes y proveedores, comunidad local y sociedad.

Para establecer el contexto de gestión de riesgos, es fundamental definir cómo el Proceso de Gestión de Riesgos se integrará y coordinará con otros sistemas de gestión existentes en la organización. Asimismo, es necesario comprender cómo se gestionan actualmente los riesgos y realizar una revisión exhaustiva de los marcos, herramientas, procesos y roles asociados a la gestión de riesgos.

Como una fuente de información para el establecimiento del contexto interno y externo, se sugiere utilizar como insumo los análisis que se han realizado en la organización gubernamental,

en el marco del control de gestión, en las Definiciones Estratégicas (ver Instrucciones para la Formulación - Formulario A1 Ficha de Definiciones Estratégicas DIPRES), ya que en ese ámbito, se han examinado y definido la misión ministerial e institucional, visión, ley orgánica, programas, ejes estratégicos, productos, clientes, indicadores, etc. Otros insumos que pueden utilizarse son la evaluación comprehensiva del gasto, la evaluación de programas, la evaluación de impacto, entre otros antecedentes.

En forma adicional, deben incorporarse en un Proceso de Gestión de Riesgos, una política de gestión de riesgos, la definición de roles y sus responsables y un diccionario de riesgos.

a. Establecer la Política de Gestión de Riesgos

La Política de Gestión de Riesgos constituye la declaración formal de la máxima autoridad del servicio respecto de las intenciones, principios y orientaciones estratégicas que regirán la identificación, análisis, evaluación, tratamiento y supervisión de los riesgos institucionales.

En concordancia con los principios establecidos en la GGSAI N°3, el enfoque de gobernanza y aseguramiento basado en riesgos promovido por Instituto de Auditores Internos (IIA) y la Política de Gestión de Riesgos deberá:

- Integrar explícitamente la gestión de riesgos al sistema de control interno, a la planificación estratégica y a la toma de decisiones institucional.
- Reconocer que la gestión de riesgos es un componente esencial del deber de control y de la responsabilidad directiva.
- Establecer el compromiso de la alta dirección con una gestión preventiva, sistemática y documentada de los riesgos.

La Política deberá ser formalmente aprobada por la máxima autoridad del servicio y contener, al menos, los siguientes elementos:

- El propósito y alcance de la gestión de riesgos, en coherencia con la misión, mandato legal y objetivos estratégicos institucionales.
- La vinculación entre la gestión de riesgos y la planificación estratégica, presupuestaria y operativa, asegurando que los riesgos estratégicos se identifiquen y gestionen como insumos para la toma de decisiones de gobernanza.
- La definición del apetito de riesgo, tolerancia al riesgo y capacidad de riesgo institucional, incluyendo criterios específicos para riesgos críticos tales como riesgos estratégicos, operacionales y de probidad administrativa, conforme a lo establecido en el presente Documento Técnico.
- La definición clara de roles, responsabilidades y obligaciones de rendición de cuentas en materia de gestión de riesgos, incluyendo el rol de la máxima autoridad, el comité de riesgos (cuando exista), las jefaturas y la función de auditoría interna.
- Los lineamientos para la gestión de conflictos de interés y otras situaciones que puedan comprometer la objetividad en la toma de decisiones relacionadas con riesgos.
- El compromiso de asignar los recursos humanos, técnicos y financieros necesarios para la implementación y mejora continua del sistema de gestión de riesgos.
- Los mecanismos de medición, seguimiento y reporte del desempeño del sistema de gestión de riesgos, incluyendo indicadores, informes periódicos y mecanismos de supervisión.

- El compromiso de revisión periódica de la política y del marco de gestión de riesgos, tanto en ciclos regulares como ante cambios relevantes en el entorno institucional, normativo o estratégico.

La Dirección deberá asegurar que la Política de Gestión de Riesgos sea coherente con la política de control interno, probidad y calidad institucional, y que sea debidamente difundida en todos los niveles organizacionales. Asimismo, deberá establecer mecanismos formales para su comunicación, implementación y actualización, garantizando trazabilidad, responsabilidad y evidencia documental.

En **Anexo Nº 6** se entrega un ejemplo de política de gestión de riesgos.

b. Establecer los Responsables y sus Roles

Se deben definir, documentar y aprobar los roles de las personas relacionadas con la Gestión de Riesgos en la organización, se debe garantizar claridad en las funciones y responsabilidades, abordando los siguientes aspectos clave:

- **Identificación de Roles Clave**

- Identificar todas las funciones necesarias para el Proceso de Gestión de Riesgos, incluyendo roles estratégicos, operativos y de soporte.
- Clasificar los roles según su nivel de influencia y responsabilidad (ejemplo: responsables de decisión, supervisión y ejecución).

- **Definición de Responsabilidades**

Establecer de manera clara y detallada las responsabilidades de cada rol, asegurando que estén alineadas con los objetivos organizacionales.

Incluir tareas específicas relacionadas con:

- Identificación y análisis de riesgos.
- Implementación de medidas preventivas o correctivas.
- Supervisión y reporte del estado de los riesgos.
- Provisión de soluciones y monitoreo de resultados

En **Anexo Nº 7**, se presenta un ejemplo de asignación de roles y responsabilidades.

Es importante señalar que el Auditor Interno de la organización gubernamental no puede ser nombrado como responsable en estos temas, ya que se estaría afectando su objetividad e independencia al momento de auditar el funcionamiento y efectividad del Proceso de Gestión de Riesgos (actividad de aseguramiento). En **Anexo Nº 8** se entrega un resumen del rol de la auditoría interna en un Proceso de Gestión de Riesgos en el sector gubernamental, destacándose aquellas funciones que puede realizar y aquellas que no le están permitidas[8].

[8] Se hace de acuerdo con la mirada del Instituto de Auditores Internos Global (IIA).

c. Establecer un Diccionario de Riesgos

A nivel teórico y práctico se considera la necesidad de formular un diccionario de riesgos para la entidad. En este caso, como se trata de organizaciones gubernamentales, el diccionario de riesgos publicado por el CAIGG es útil como referencia para todas las organizaciones del Sector Público.

1.3. Criterios

Cada entidad debe precisar la cantidad y el tipo de riesgo que puede o no puede tomar (Apetito de Riesgo), para lograr los objetivos y para apoyar los procesos de toma de decisiones. Considerando lo anterior, se deben definir los criterios para valorar la importancia del riesgo a través de su nivel de probabilidad e impacto y su nivel de exposición al riesgo, entre otras variables.

El **Anexo N° 9 (Criterios: Tablas de Valuación para Construir la Matriz de Riesgos)** contiene una definición global y transversal para determinar los niveles de riesgos que se pueden tomar en las entidades públicas determinada por el CAIGG.

2. Fase: Evaluación del Riesgo

La evaluación del riesgo debe realizarse de manera sistemática, iterativa y colaborativa, asegurando que el proceso sea estructurado, basado en evidencia y alineado con los objetivos organizacionales. Para lograr una evaluación efectiva, es fundamental considerar los siguientes aspectos:

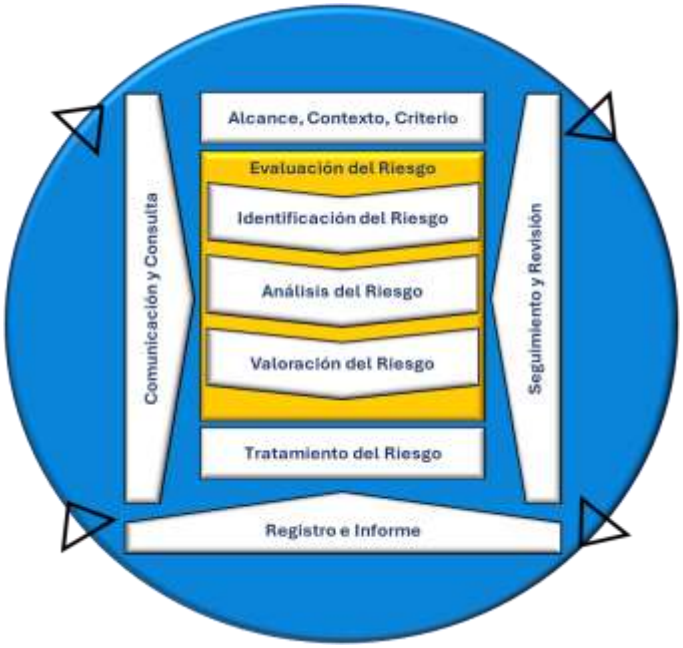
- **Enfoque Sistemático**
  - La evaluación del riesgo debe seguir un método estructurado y documentado, asegurando que se apliquen criterios homogéneos en todo el proceso.
  - Se deben definir parámetros claros para la identificación, análisis y valoración del riesgo, garantizando la coherencia en la toma de decisiones.

- **Proceso Iterativo**
  - La evaluación de riesgos no es un proceso estático, sino que debe ser periódicamente actualizado y ajustado en función de nuevas amenazas, cambios en el entorno o información emergente.
  - Los escenarios y análisis de riesgos deben ajustarse a la evolución de la organización y su entorno estratégico.

- **Enfoque Colaborativo y Participativo**
  - Se debe involucrar a las partes interesadas relevantes, asegurando que la evaluación del riesgo refleje una visión integral y no solo la percepción de un grupo reducido.
  - La participación de diferentes actores permite considerar múltiples perspectivas y experiencias, enriqueciendo el análisis y fortaleciendo la toma de decisiones.

- **Uso de la Mejor Información Disponible**
    - La evaluación del riesgo debe basarse en datos y evidencia actualizada, garantizando que las decisiones se fundamenten en información confiable.
    - En caso de incertidumbre o falta de datos, se debe complementar con investigación adicional, consulta de expertos o análisis de tendencias.

Figura N° 6: Fase Evaluación del Riesgo



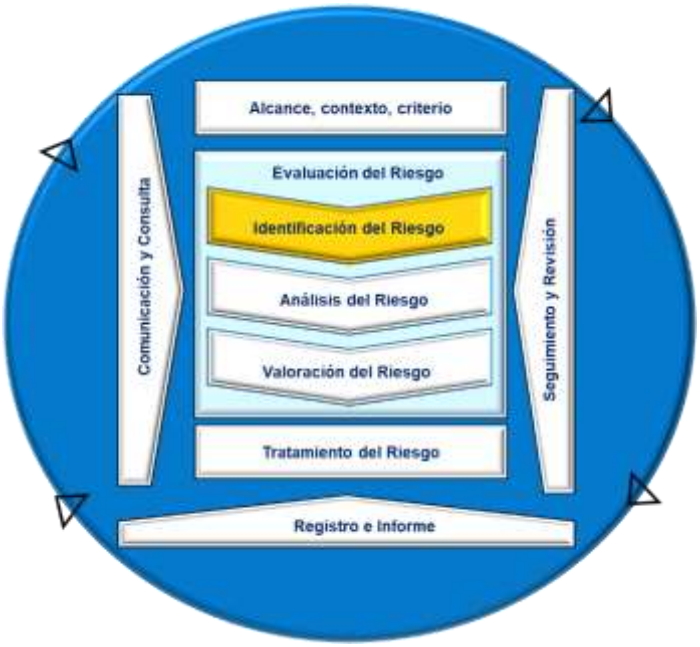
Fuente: NCh-ISO 31000:2018 – INN

Una evaluación de riesgos efectiva permite a las organizaciones gubernamentales anticiparse a amenazas, optimizar la toma de decisiones y fortalecer su capacidad de resiliencia. Al aplicar un enfoque sistemático, iterativo y colaborativo, fundamentado en la mejor información disponible, se garantiza que la gestión de riesgos sea un pilar estratégico en la administración pública y en la mejora continua de los procesos organizacionales

La metodología del CAIGG, considera la identificación, análisis y valoración de riesgos y oportunidades que pueden afectar la consecución de los objetivos estratégicos de la organización gubernamental. Las oportunidades y riesgos son eventos, que se definen como un incidente que emana de fuentes internas o externas que afectan la implementación de la estrategia o logro de los objetivos.

2.1. Sub-Fase Identificación del Riesgo

Figura N° 7: Sub-Fase Identificación de Riesgos



Fuente: NCh-ISO 31000:2018 – INN

Los eventos pueden generar impactos positivos o negativos, o ambos. Los impactos positivos, se denominan oportunidades, y los negativos son conocidos como riesgos.[9] El riesgo es el efecto de la incertidumbre sobre el objetivo.[10]

Como puede apreciarse, la identificación de eventos consta de dos aspectos, oportunidades y riesgos.

a. Identificación de Oportunidades

Un aspecto importante que considerar al identificar oportunidades es la existencia de eventos que pueden producir efectos negativos y positivos a la vez, por ejemplo, la prioridad que le da el Gobierno a ciertos programas produce el efecto positivo de tener mayores recursos y mayor apoyo para desarrollarlos, pero a la vez podría eventualmente producir una mayor exposición de estos a la opinión pública.

La identificación de oportunidades es de vital importancia para retroalimentar las estrategias en la organización, siendo también relevante para orientar el tratamiento de los riesgos, por lo que éstas deben ser conocidas y evaluadas oportunamente por la dirección de la organización gubernamental.

[9] De acuerdo con COSO ERM, los eventos son todas aquellas circunstancias que pueden afectar la consecución de los objetivos estratégicos de una organización. Las que lo afectan en forma positiva se denominan oportunidades y las que afectan en forma negativa, se denominan riesgos.
[10] NCh-ISO 31000:2018.

A continuación, en el **Cuadro Nº 7** se entrega un ejemplo de identificación de oportunidades a través de eventos.

Cuadro Nº 7: Ejemplo de Identificación de Oportunidades por Proceso

Entidad	Misión	Procesos	Eventos/Oportunidades
Servicio Apoyo al Microcrédito (ficticio).	Entregar apoyo crediticio de fomento a grupos vulnerables, de mujeres y jóvenes.	Sistema Crediticio de Fomento	• Está dentro de los lineamientos del nuevo Gobierno. • Cambios sociales que apuntan a un papel protagónico de la mujer. • La mujer estadísticamente es más cumplidora y responsable con sus deudas y compromisos. • Se han aumentado los fondos para apoyar a microempresarias afectadas por el terremoto.
		Apoyo a la Capacitación	• La mujer en general, es responsable en asistencia a los cursos. • Los jóvenes reclaman alternativas de mejoramiento. • En los últimos años ha existido una gran demanda por capacitación. • Existen muchos organismos técnicos en el mercado que ofrecen diversas alternativas. • El presupuesto de este año contempla más recursos que el año anterior para este proceso.
		Recursos Humanos	…..
		Sistemas de Información	…..
		Contabilidad y Presupuesto	…..

b. Identificación del Riesgo (Paso N° 7 en la Matriz de Riesgos)

La identificación de eventos que pueden impactar negativamente el cumplimiento de los objetivos organizacionales es un paso clave dentro del Proceso de Gestión de Riesgos. Este análisis permite anticipar amenazas, minimizar su impacto y, en algunos casos, aprovechar oportunidades derivadas del entorno operativo y estratégico. En el **Anexo Nº 10** se acompañan ejemplos de técnicas de identificación de eventos generadores de riesgos y oportunidades.

Una vez identificados los objetivos operativos correspondientes a etapas o subprocesos relevantes, según sea la máxima desagregación de los procesos donde se realizará el levantamiento, es necesario identificar los riesgos relevantes que se presentan asociados a los objetivos en cada proceso crítico, subproceso y etapa, entendiendo como tales a la incertidumbre sobre los objetivos operativos, así como a la posibilidad (probabilidad) de que un acontecimiento ocurra y afecte (consecuencia o impacto) negativamente a la consecución total o parcial de los objetivos operativos. En **Anexo Nº 11**, se presenta los pasos recomendados para describir y redactar riesgos.

c. Fuente y Tipología de Riesgos (Paso N° 8 en la Matriz de Riesgos)

La fuente del riesgo es un elemento clave en la gestión de riesgos, ya que permite entender el origen de los eventos que pueden afectar el cumplimiento de los objetivos estratégicos y operacionales de una organización gubernamental. Los riesgos pueden clasificarse según su fuente u origen en riesgos de fuente externa y riesgos de fuente interna.

Los riesgos de fuente externa son aquellos que provienen de factores fuera del control de la organización gubernamental. Su gestión se centra en la capacidad de anticipación, adaptación y respuesta, ya que la entidad no puede evitar su ocurrencia, pero sí puede minimizar sus efectos. Dado que estos riesgos están fuera del control directo de la organización, la clave está en la anticipación y el plan de respuesta. Estrategias como la planificación de escenarios, la resiliencia organizacional y la gestión de crisis pueden ayudar a minimizar su impacto.

Los riesgos de fuente interna tienen su origen dentro de la propia organización gubernamental y están relacionados con su estructura, procesos, recursos humanos y sistemas internos. A diferencia de los riesgos externos, estos sí pueden ser gestionados y mitigados directamente mediante controles y mejoras en la organización. Dado que estos riesgos pueden ser controlados dentro de la organización, la estrategia de mitigación se centra en la implementación de controles internos efectivos, capacitación del personal, fortalecimiento de la gobernanza y automatización de procesos para minimizar errores y mejorar la eficiencia.

Por otra parte, en el marco del levantamiento de procesos, debe utilizarse una tipología o categorización de riesgos. En estas categorías deben clasificarse los riesgos operativos que se identifiquen en la próxima fase. La tipología de riesgos es un mecanismo de clasificación que permite agrupar los riesgos según sus características, naturaleza o impacto en la organización. Esta clasificación facilita su análisis, monitoreo y tratamiento dentro del Proceso de Gestión de Riesgos, asegurando un enfoque estructurado para la toma de decisiones.

En el **Cuadro Nº 8**, se incluyen ejemplos de los tipos de riesgos, considerando los elementos que caracterizan a cada uno. Es necesario indicar que la clasificación propuesta es una adaptación de la establecida en el Marco COSO ERM, que se ha modificado para ser aplicada en la metodología de Gestión de Riesgos emitida por el CAIGG.

Cuadro Nº 8: Ejemplos de Tipología de Riesgos

Tipos de Riesgos	Elementos que los Caracteriza	Ejemplos de Riesgos Específicos
Financieros	Se relacionan con el uso adecuado de los recursos entregados por el Estado a sus organizaciones	- Mal uso de los recursos - Desviación de recursos - Entrega de recursos a no beneficiarios - Malversación de fondos - Uso de recursos con fines distintos a los aprobados
Económicos	Se relacionan con elementos financieros, comerciales y presupuestarios	- Falta de disponibilidad presupuestaria - Modificaciones presupuestarias por deficiente ejecución - Errores en el servicio de la deuda - Servicio de la deuda muy alto - Exceso de compromisos de la Organización Gubernamental que afecten su presupuesto - Malas inversiones en mercado de capitales - Deficiencias en la ejecución presupuestaria de la Organización Gubernamental - Falta de Suplementos del Ministerio de Hacienda o falta de oportunidad en los mismos.
Sociales	Se relacionan con elementos de comunidad social, cultural,	- Deficiente comportamiento de usuarios (bajo compromiso, bajo cumplimiento, etc.)

Tipos de Riesgos	Elementos que los Caracteriza	Ejemplos de Riesgos Específicos
	demográfica, comportamientos sociales.	- Problemas con los datos personales y privados de los clientes o proveedores - Falta de responsabilidad social de la Organización Gubernamental o excesivamente gravosa - Cambios culturales en los usuarios de la Organización Gubernamental (bajo interés, dificultades para aplicar políticas, etc.)
Tecnológicos	Acerca de las tecnologías de la información como concepto y los cambios que producen a nivel global en el sector o la Organización Gubernamental	- Interrupción de servicios - Complejidades del Comercio Electrónico gravosas para la Organización Gubernamental - Complejidades y requisitos del Gobierno Electrónico - Falta de cumplimiento de las obligaciones emanadas del Gobierno Electrónico - Falta de confiabilidad de los datos externos - Desactualización de la Organización Gubernamental debido a las tecnologías emergentes - Falta de poder adquisitivo de la Organización Gubernamental frente a las nuevas tecnologías.
Estratégicos	Aspectos claves para el desarrollo de la Organización Gubernamental, que se relaciona con decisiones superiores y política de Gobierno	- Falta de planificación en los cambios de gobierno - Deficiencias en el conocimiento, comprensión y aplicación de las políticas públicas por parte de la Organización Gubernamental - Nuevas regulaciones y tarifas dificultan el quehacer institucional o lo hacen más gravoso
Medioambientales	Aspectos que afectan la calidad del medioambiente, sean ocasionados por el hombre o la naturaleza	- Falta de cumplimiento normativo en las emisiones y residuos - Dificultades con el uso de la energía - Situaciones producidas por catástrofes naturales - Falta de garantías de desarrollo sustentable - Malas decisiones de impacto medioambiental
Procesos	Elementos que se relacionan con los distintos aspectos de los procesos que desarrolla la Organización Gubernamental; como el diseño, la ejecución, la supervisión y los clientes	- Deficiencias en el diseño del proceso - Ejecución errónea de los procesos - Ejecución inoportuna de los procesos - Falta de supervisión - Falta de responsables de ejecutar la supervisión y monitoreo - Falta de medidas adoptadas ante la supervisión, o se adoptan medidas que no son adecuadas - Falta de cumplimiento o deficiencias en el mismo por parte de los clientes
Legal	Aspectos de cumplimiento y de conformidad del actuar de la Organización Gubernamental con la normativa pública general y específica aplicable a ésta.	- Falta de actualización por cambios en la legislación - Aumento de los requerimientos por cambio de legislación - Falta de cumplimiento de normas por deficiencias en las mismas (normas oscuras o contradictorias, vacíos legales)
Personas	Aspectos relacionados al personal de la Organización Gubernamental, desde su ingreso hasta su egreso del mismo.	- Falta de capacidad del personal - Personal sin capacitación - Actividad fraudulenta del personal - Deficiencias en la seguridad e higiene y en el ambiente de trabajo de la Organización Gubernamental. - Deficiencias en el cumplimiento de normas de personal (dotación, escalafón, etc.)

Tipos de Riesgos	Elementos que los Caracteriza	Ejemplos de Riesgos Específicos
Imagen	Aspectos relacionados con el perfil de la Organización Gubernamental y la reputación social del mismo. Percepción de la comunidad del actuar de la Organización Gubernamental	- Escándalos - Corrupción - Incumplimiento de las funciones de la Organización Gubernamental - Disconformidad de los usuarios - Mal uso de recursos
Sistemas	Relacionado con los sistemas de información de la Organización Gubernamental, las tecnologías que posee y los datos que maneja.	- Falta de integridad y confiabilidad de datos - Falta de disponibilidad de datos y sistemas - Deficiencias en la selección de sistemas - Deficiencias en el desarrollo y despliegue de los sistemas - Deficiencias en el mantenimiento - Falta de interoperabilidad de los sistemas
Bienes muebles e inmuebles	Se relacionan con elementos asociados a los recursos materiales muebles o bienes raíces que utiliza la Organización Gubernamental para el cumplimiento de sus objetivos institucionales.	- Excesiva antigüedad de los bienes - Difíciles condiciones de protección de los bienes - Vulnerabilidad de los bienes ante el uso o ante elementos externos que aceleran su deterioro - Incumplimiento o falta de planes de protección y resguardo de bienes - Desaparición física de bienes, el deterioro de los bienes que imposibiliten cumplir su función - Mal uso de los bienes o en forma distinta a su naturaleza

Esta tipología de riesgos es complementaria y afín de lo indicado en la GGSAI Nº 3.

La tipología de riesgos es una herramienta clave en la gestión de riesgos, ya que permite ordenar y estructurar los riesgos dentro de una organización. La correcta clasificación y análisis de estos riesgos facilita la priorización de acciones preventivas, optimiza la asignación de recursos y fortalece la capacidad de resiliencia organizacional.

d. Señales de Alerta para Delitos LA/FT/DF, asociadas a los riesgos (Paso N° 9 en la Matriz de Riesgos) pasar a Riesgos de Integridad

Este punto del documento ha sido formulado con el aporte de los especialistas de la Unidad de Análisis Financiero (UAF), con la finalidad de generar un procedimiento que permita cumplir con los requerimientos del Oficio Circular N° 20/2015 del Ministerio de Hacienda, respecto de velar por la inclusión de los riesgos relacionados con el Sistema Preventivo y los derivados de los cambios sobre Delitos LA/FT/DF, en los mapas de riesgos institucionales.

- Para cada riesgo identificado en la Matriz de Riesgos Estratégica, se deberá asociar, si corresponde, señales de alerta para delitos LA/FT/DF[11]. También debe identificarse el o los cargos de los funcionarios que se relacionen teóricamente con la señal de alerta. Para realizar dicha labor se sugiere revisar los siguientes antecedentes:

[11] Las señales de alerta de delitos LA/FT/DF se pueden concebir como; indicadores, indicios, condiciones, comportamientos o síntomas de ciertas operaciones o personal que podrían permitir potencialmente detectar la presencia de una operación sospechosa de lavado de activos, delitos funcionarios o financiamiento del terrorismo (Adaptado de definiciones realizadas por la Unidad de Análisis Financiero (UAF), ver **Anexo N° 12**.

- **Anexo N° 12**. Conceptos sobre delitos de Lavado de Activos (LA), Financiamiento del Terrorismo (FT) y Delitos Funcionarios (DF). Este contiene conceptos, descripciones y definiciones básicas sobre los delitos con los cuales se relacionan las señales de alerta.
- **Anexo N° 13**. Ejemplos de señales de alerta genéricas para delitos LA/FT/DF. Este contiene, solo a modo de ejemplo, algunas banderas rojas o señales de alerta genéricas, que se pueden identificar en las actividades operativas en cualquier organización y que pueden ser indicativas, debiendo examinarse detalladamente para ver si corresponden a situaciones anómalas. Sin perjuicio de lo anterior, las señales de alerta siempre deben ser identificadas y analizadas de acuerdo con el contexto del sector donde está incorporada la organización.
- Guía Señales de Alerta, publicada en la página web de la Unidad de Análisis Financiera (UAF); http://www.uaf.gob.cl/entidades/tipo_senales.aspx
- Oficio Circular N° 20/2015 del Ministerio de Hacienda. Orientaciones generales para el Sector Público en relación al inciso sexto del artículo 3° de la ley N° 19.913.
- Guía de Recomendaciones para el Sector Público en la implementación de un sistema preventivo contra los delitos funcionarios, el lavado de activos y el financiamiento del terrorismo (Adjunta al Oficio Circular N° 20/2015 del Ministerio de Hacienda).
- Material del curso E-Learning para prevenir el lavado de activos y el financiamiento del terrorismo en las Instituciones Públicas, entregado por la Unidad de Análisis Financiero (UAF).

- Sin perjuicio de las señales de alerta de delitos LA/FT/DF incluidas en la Matriz de Riesgos Estratégica, se deberá adicionalmente:

  - Identificar riesgos o señales de alerta LA/FT/DF en los procesos, subprocesos, etapas, proyectos, sistemas, etc. que no hayan sido considerados en la Matriz de Riesgos Estratégica, por no estar dentro del porcentaje mínimo (valor porcentual mínimo) de procesos críticos que deben analizarse en la organización, según lo informado por el CAIGG. En el caso que todos los procesos de la Organización estén incluidos en la Matriz de Riesgos Estratégica, no será necesario considerar este requerimiento.
  - Identificar cuando sea posible, otras señales de alerta de delitos LA/FT/DF relacionados con procesos, subprocesos, etapas, etc. que por su naturaleza y características, no se han podido asociar a los riesgos operativos incluidos en la Matriz de Riesgos Estratégica. Se recomienda ver ejemplos en **Anexo N° 13**.

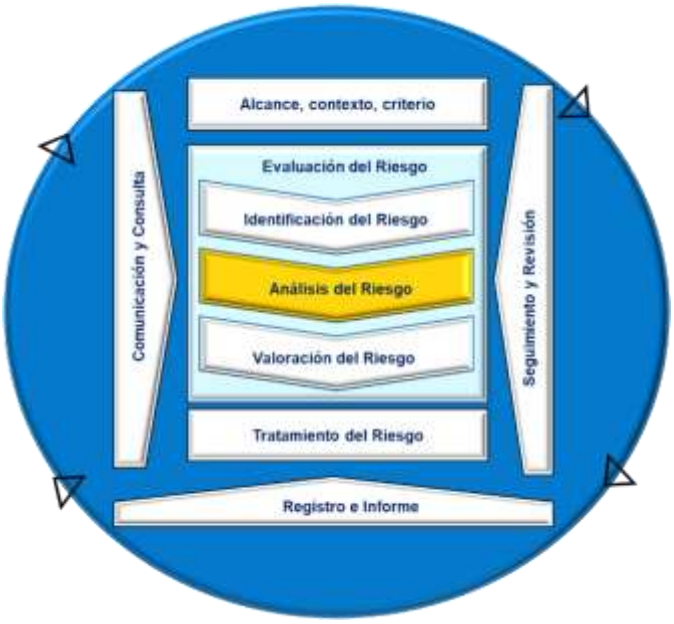
Para levantar la información y comunicar el resultado del análisis de los requerimientos del punto anterior al CAIGG, se debe cumplir con lo dispuesto en el **Anexo N° 14**. Señales de Alerta LA/FT/DF No Asociadas con los Riesgos Incluidos en la Matriz de Riesgos Estratégica.

2.2. Sub-Fase Análisis del Riesgo

Esta fase busca comprender la naturaleza de cada riesgo identificado, estimando su nivel de probabilidad y potencial impacto, considerando los controles existentes. Este análisis proporciona información crítica para:

- Priorizar los riesgos,
- Decidir si requieren tratamiento,
- Y definir las estrategias más adecuadas para su gestión.

Figura N° 8: Sub-Fase Análisis del Riesgo



Fuente: NCh-ISO 31000:2018 – INN

Las principales actividades que se deben desarrollar para un adecuado análisis del riesgo esquemáticamente son las siguientes:

- Evaluar la probabilidad de ocurrencia.
- Estimar el impacto potencial, considerando múltiples dimensiones.
- Analizar la existencia, cobertura y eficacia de los controles actuales.
- Determinar los niveles de riesgo inherente y residual.
- Identificar supuestos, incertidumbres, sesgos o limitaciones.
- Documentar todo el proceso de análisis.

Por otra parte, el análisis del riesgo puede estar influenciado por diversos factores que deben ser considerados, documentados y comunicados:

- Divergencia de opiniones entre participantes del proceso.
- Sesgos cognitivos y organizacionales.
- Percepciones individuales del riesgo.
- Juicios subjetivos que puedan afectar la objetividad.
- Calidad y disponibilidad de la información utilizada.
- Supuestos técnicos, vacíos de datos o exclusiones explícitas.
- Limitaciones metodológicas y de ejecución de las técnicas empleadas.

Estas influencias deben ser registradas como parte del proceso, ya que afectan la confiabilidad del análisis y las decisiones posteriores.

Las organizaciones gubernamentales deberán poner al día su análisis de riesgos, en base a los criterios definidos en este documento técnico, actualizando la Matriz de Riesgos Estratégica de la entidad y considerando en forma especial todos aquellos procesos nuevos que desarrolle la organización, con sus respectivos riesgos y controles, analizando especialmente los riesgos nuevos y los nuevos énfasis de Gobierno que han definido los Jefes de Servicio y otras autoridades.

a. Probabilidad e Impacto (Paso N° 10 en la Matriz de Riesgos)

Para ello se debe proceder a la medición (nivel de severidad del riesgo, de acuerdo con los criterios definidos en la escala presentada en el **Anexo Nº 9**). Evaluando en términos de su probabilidad, como posibilidad de ocurrencia del riesgo potencial y de su impacto, como consecuencia que puede ocasionar a la organización la materialización del riesgo. Lo anterior nos va a entregar la severidad del riesgo y su clasificación, de acuerdo con la matriz de impacto y probabilidad (Mapa de Calor) que se expone más adelante en este documento.

b. Ajuste cualitativo de Severidad

La severidad podrá ajustarse mediante evaluación cualitativa de:

- Vulnerabilidad institucional.
- Velocidad de materialización.
- Interdependencia con otros procesos.
- Correlación con otros riesgos.
- Impacto en el valor público.

Severidad Ajustada = Severidad Base × Multiplicador Cualitativo

Este ajuste evita subestimar riesgos que, aun con baja probabilidad, pueden comprometer gravemente la legitimidad institucional. Los aspectos de detalle se encuentran definidos y ejemplificados en el **Anexo Nº 1.**

c. Reconocimiento y Levantamiento de los Controles Claves (Paso N° 11 en la Matriz de Riesgos)

El siguiente paso consiste en el reconocimiento y levantamiento de los controles existentes en la organización gubernamental, orientados a mitigar los riesgos identificados.

En esta etapa deberá efectuarse un análisis crítico de los controles, relevando exclusivamente aquellos que tengan carácter clave y cuya finalidad sea reducir la probabilidad de ocurrencia o el impacto del riesgo.

El **Anexo Nº 15** desarrolla los aspectos conceptuales y estructurales del control, conforme a lo establecido en las GGSAI.

Por su parte, el **Anexo Nº 16**, “Conceptos Generales sobre Requisitos Básicos de Control Adecuado considerados en el Modelo”, establece los criterios técnicos que permiten operativizar la identificación, evaluación y validación de los controles levantados, determinando cuándo un

control puede considerarse adecuadamente diseñado para efectos de la gestión del riesgo y su posterior aseguramiento.

Deben clasificarse y calificarse los controles, de acuerdo con su nivel de cumplimiento con los elementos de un control adecuado especificados en el modelo y según su oportunidad, periodicidad y automatización, utilizando para ello la metodología del CAIGG (los criterios para valuación se presentan en el **Anexo Nº 9**).

Luego, se debe calcular el nivel de exposición al riesgo, que corresponde al nivel de riesgo una vez considerada la calificación y valoración de los controles. El nivel de exposición al riesgo se determinará por riesgo, por etapa, por subproceso y por proceso (criterios para valuación se presentan en el **Anexo Nº 9**). En forma adicional, se debe calcular el riesgo ponderado por subproceso.

d. Determinación del Nivel de Criticidad del Riesgo Inherente (Severidad del Riesgo)

Es el resultado de combinar la probabilidad, el impacto (y las dimensiones adicionales del riesgo, si así se hubiera decidido en la organización), sin considerar el efecto de los controles existentes. Esta valoración puede realizarse mediante métodos cuantitativos, cualitativos o mixtos. Se recomienda:

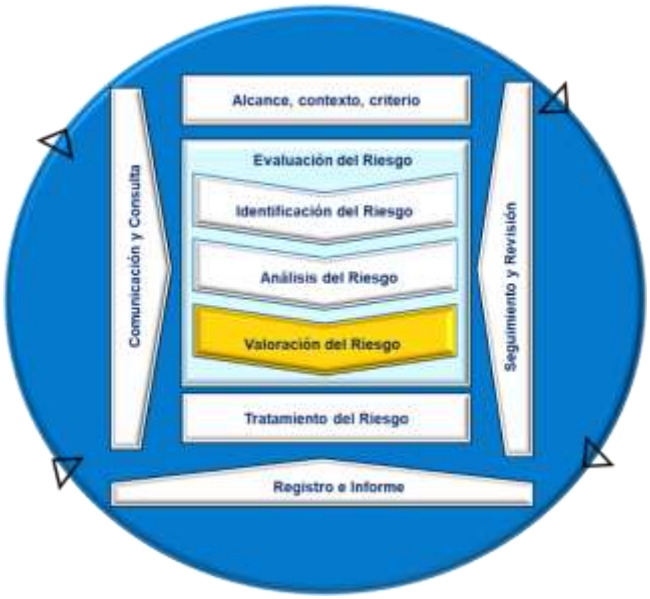
- Aplicar escalas consistentes y previamente definidas.
- Asignar ponderaciones cuando se desee priorizar alguna dimensión (por ejemplo, dar mayor peso al impacto).
- Documentar claramente la metodología usada, asegurando la trazabilidad y comparabilidad de los resultados.

2.3. Sub-Fase Valoración del Riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.

En la metodología la Fase de Valoración de los Riesgos considera dos pasos. Primero la definición y confirmación del criterio que se escogerá (definido en la Fase de Definición del Contexto de la Gestión de Riesgos) y segundo la confección de un ranking de riesgos en la organización.

Figura N°9: Sub-Fase Valoración del Riesgo



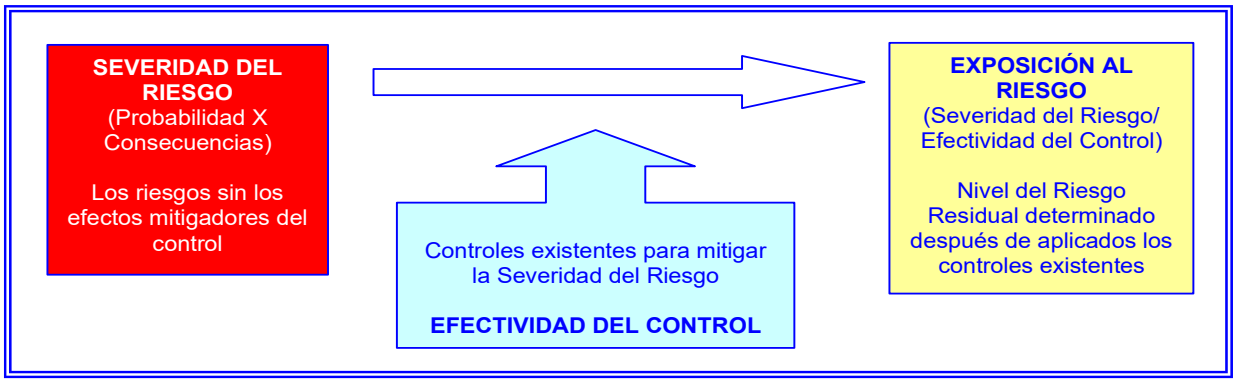
Fuente: NCh-ISO 31000:2018 – INN

a. Definición y Confirmación de Criterios para Ranking

En el caso de los Procesos se utilizará como criterio para la confección del Ranking, el nivel de exposición al riesgo de estos. En cuanto a los subprocesos, se utilizará el criterio asociado al nivel de exposición al riesgo ponderada, esto es, el riesgo residual que subsiste después de aplicados todos los controles claves existentes. Para un adecuado desarrollo del Proceso de Gestión de Riesgos, el nivel de exposición al riesgo debe considerar la ponderación estratégica de subprocesos, de acuerdo con lo señalado en los párrafos anteriores. Esto implica que el criterio considerado para la evaluación del riesgo es el de exposición al riesgo ponderada para los subprocesos (exposición al riesgo x ponderación estratégica). Esta evaluación se determina considerando los niveles de exposición al riesgo de las etapas de acuerdo con el promedio aritmético de los riesgos específicos de contiene cada una de las etapas del Subproceso.

En la **Figura Nº 10** que se presenta a continuación, se muestra la relación entre los distintos componentes del análisis de riesgos.

Figura Nº 10: Relación entre Severidad del Riesgo y Exposición al Riesgo



b. Evaluación del Riesgo Residual o Exposición al Riesgo, Comparación con el Apetito de Riesgo y Respuesta al Riesgo

Una vez estimado el riesgo inherente se deben:

- Efectuar el ajuste cualitativo de Severidad
- Identificar los controles clave existentes para mitigar el riesgo.
- Evaluar su diseño y efectividad operativa.
- Determinar el nivel de exposición al riesgo o riesgo residual (riesgo remanente tras aplicar los controles).
- Este nivel se compara con el apetito de riesgo institucional, es decir, con el nivel de riesgo que la organización está dispuesta a aceptar para cumplir sus objetivos.
    - Si el riesgo residual está dentro del apetito, se considera aceptable y no se requiere acción adicional.
    - Si el riesgo residual excede el apetito, se considera no aceptable, por lo que deben tomarse medidas: reforzar controles, reformular acciones correctivas o escalar a la Alta Dirección y/o Jefe de Servicio.

- Complementariamente, deberá documentar y evaluar la razonabilidad de las respuestas adoptadas por la Dirección, asegurando que sean proporcional al nivel de exposición de los riesgos.

c. Incorporación del Concepto de Ponderación Estratégica

Debe aplicarse el concepto de ponderación estratégica a nivel de subproceso para cada proceso crítico. En efecto, para determinar el nivel de exposición al riesgo ponderada de los subprocesos, deberá multiplicarse el nivel de exposición al riesgo de cada subproceso por el porcentaje de ponderación estratégica que a cada uno de ellos le fue asignado, de la forma que se explica en el **Cuadro N° 9** a continuación:

Cuadro Nº 9: Ejemplo de Ponderación Estratégica por Subprocesos

Proceso Transversal	Proceso	Subproceso	Pon[12]	Etapas	...	Nivel de Exposición al Riesgo (Riesgo Residual)				Nivel de Exposición al Riesgo Ponderada
						Riesgo Específico	Etapa	Subproceso	Proceso	Subproceso
Proceso Transversal 1	Proceso 1	Subproceso 1	70%	Etapa 1		3	3	3	2,8	3 x 70% = **2,1**
				Etapa 2		3	3			
		Subproceso 2	30%	Etapa 3		3	3	2,5		2,5 x 30% = **0,75**
				Etapa 4		2	2			
Proceso Transversal 2	Proceso 2	Subproceso 3	60%	Etapa 5		5	5	3,5	3,8	3,5 x 60% = **2,1**
				Etapa 6		2	2			
		Subproceso 4	40%	Etapa 7		2	2	4		4 x 40% = **1,6**
				Etapa 8		6	6			
Proceso Transversal 3	Proceso 3	Subproceso 5	50%	Etapa 9		2	2	2	2,7	2 x 50% = **1**
				Etapa 10		2	2			
		Subproceso 6	50%	Etapa 11		2	2	3,3		3,3 x 50% = **1,65**
				Etapa 12		4	4			
				Etapa 13		4	4			

Del **Cuadro Nº 9**, es posible apreciar que la ponderación estratégica releva la importancia del proceso en el contexto de la Institución y del subproceso en el contexto del proceso, acercando el resultado a la posición y relevancia de éstos.

d. Ranking de Riesgos

Basado en la información contenida en la Matriz de Riesgos Estratégica de la organización gubernamental construida en las fases anteriores del proceso, se debe evaluar en cuáles ámbitos organizacionales se requiere actuar en forma prioritaria (procesos, subprocesos y etapas).
Para dar cumplimiento a esta tarea, la organización debe construir un Ranking de Riesgos en base al nivel de exposición al riesgo para los procesos críticos (promedio aritmético de la exposición al riesgo de los subprocesos) y en base al nivel de exposición al riesgo ponderado para los subprocesos que componen dichos procesos:

- **Ranking de Procesos por Nivel de Exposición al Riesgo**

En **el Cuadro Nº 10** se presenta el esquema del análisis a realizar para un proceso crítico que fue desagregado hasta el nivel de riesgo operativo.

Cuadro Nº 10: Ejemplo de Ranking de Procesos por Nivel de Exposición al Riesgo

Procesos	Nivel de Exposición al Riesgo (Riesgo Residual)	Ranking para priorizar estrategias de tratamiento de los riesgos en los Procesos Críticos
Entrega Créditos	4,0	1º
Capacitación	3,5	2º
Contabilidad y Presupuesto	3,0	3º
……	….	….

De lo anterior, se deduce que la organización gubernamental comenzará a definir y aplicar estrategias para efectuar el tratamiento de los riesgos asociados al proceso con mayor nivel en el ranking, es decir, en el ejemplo comenzará por el "Proceso de Entrega de Créditos", seguirá con el de "Capacitación" y así sucesivamente.

- **Ranking de Subprocesos por Nivel de Exposición al Riesgo (Riesgo Residual) Ponderado (ponderación estratégica)**

Una vez identificados los procesos críticos dónde se aplicarán primero las estrategias para tratar los riesgos, se deben identificar en base al nivel de exposición al riesgo ponderado, los subprocesos que componen los procesos críticos donde se aplicarán en forma prioritaria las estrategias.

Dentro de los subprocesos priorizados deben ser tratados los riesgos, correspondientes a las actividades que se desarrollan al interior de todas las etapas que los componen, priorizados de acuerdo con el nivel de exposición al riesgo para cada etapa.

De esta manera, en el ejemplo el Ranking podría aparecer como sigue, en el **Cuadro N° 11**:

Cuadro Nº 11: Ejemplo de Ranking de Subprocesos (Cuadro Considera el Ranking de Etapas por nivel de exposición al riesgo)

Procesos	Subprocesos	Nivel de Exposición al Riesgo Ponderado por Subproceso	Ranking para priorizar estrategias de tratamiento en los subprocesos	Etapas	Nivel de Exposición al Riesgo por Etapa	Ranking para priorizar estrategias de tratamiento de los riesgos en las etapas	Fundamentos para la Priorización
1° Entrega Créditos	Subproceso 1	1,8	**1°**	Etapa 1	2,1	1°	Formará Parte del Plan de Tratamiento a nivel de Subproceso y a nivel de Etapa
				Etapa 2	1,9	2°	
	Subproceso 2	1,0	**2°**	…	…	…	…
				…			
	….	….	….	…	…	…	…
				…			
	Subproceso 2	1,7	**1°**	Etapa 2	…	…	…

Procesos	Subprocesos	Nivel de Exposición al Riesgo Ponderado por Subproceso	Ranking para priorizar estrategias de tratamiento en los subprocesos	Etapas	Nivel de Exposición al Riesgo por Etapa	Ranking para priorizar estrategias de tratamiento de los riesgos en las etapas	Fundamentos para la Priorización
2° Capacitación				Etapa 1	…		
	Subproceso 1	1,0	**2°**	…	…	…	…
				…			
	….	….	….	…	…	…	…
				…			
….	….	….	….	…	…	…	No formará parte del Plan de Tratamiento por razones de costos

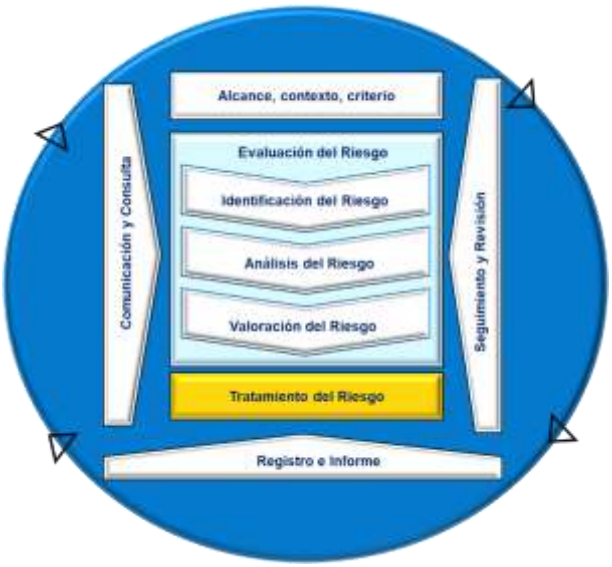
Este ranking indica que se debe comenzar a trabajar en los subprocesos 1 y 2 del proceso crítico “Entrega de Créditos”, riesgos de las etapas 1 y 2, y así sucesivamente con los demás.

3. Fase: Tratamiento del Riesgo

La Fase Tratamiento del Riesgo, implica que la dirección debe tomar todas las acciones necesarias en forma concreta para administrar los riesgos una vez que han sido analizados y priorizados en el ranking de riesgos.

Por la importancia que esta fase adquiere en un Proceso de Gestión de Riesgos en el Sector Gubernamental, se ha estimado necesario entregar algunos elementos que permitan una mejor comprensión de esta.

Figura N° 11: Fase Tratamiento del Riesgo



Fuente: NCh-ISO 31000:2018 – INN

3.1. Formular Estrategias para el Tratamiento y Monitoreo de los Riesgos

Una vez evaluados y priorizados los riesgos en las fases respectivas, la dirección debe asumir la realización de las acciones concretas necesarias para tratarlos y monitorearlos, generando una respuesta lo suficientemente adecuada para mantener la exposición del riesgo en un nivel aceptado.

Sin perjuicio de lo anterior, en los casos con niveles de exposición al riesgo de nivel “Bajo”, pese a que se identificaran controles muy efectivos en relación con el riesgo, habrá que analizar la severidad del riesgo en forma individual, en especial, el nivel de impacto que se produciría de materializarse dichos riesgos. También debe realizarse un monitoreo que permita actualizar el impacto o probabilidad oportunamente.

3.2. Estrategias Genéricas para Tratamiento de los Riesgos

La NCh-ISO 31000:2018 señala que el tratamiento del riesgo supone un proceso cíclico de:

- Evaluar un tratamiento del riesgo.
- Decidir si los niveles de riesgo residual son tolerables.
- Si no son tolerables, generar un nuevo tratamiento del riesgo.
- Evaluar la eficacia de este tratamiento.

También aclara que las opciones de tratamiento del riesgo no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias. Las opciones pueden incluir lo siguiente:

- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que causa el riesgo.
- Aceptar o aumentar el riesgo a fin de perseguir una oportunidad.
- Eliminar la fuente del riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo con otras partes (incluyendo los contratos y la financiación del riesgo)
- Retener el riesgo en base a una decisión informada.

Por su parte, los principales marcos de gestión de riesgos corporativos señalan que existen cuatro estrategias globales que permiten enfrentar la problemática de gestionar los riesgos, desde el punto de vista de su nivel de severidad (probabilidad y consecuencias) y del nivel de la exposición al riesgo (severidad – efectividad control), estas estrategias globales o genéricas son:

- **Evitar:** Salir de las actividades que generen los riesgos. Cuando esto sea realizable y no afecte los requerimientos legales o la eficiencia operacional. La aplicación de esta estrategia en el sector público está muy limitada, ya que la mayoría de su quehacer se encuentra normado en sus leyes orgánicas u otros cuerpos legales, por lo cual el salir de una actividad, generalmente no es una decisión que se pueda adoptar en forma independiente.

- **Reducir:** Implica llevar a cabo acciones para reducir la probabilidad o las consecuencias del riesgo o ambos a la vez. Adicionalmente puede analizarse si es posible mejorar la efectividad del control asociado al riesgo.

- **Compartir:** La probabilidad o las consecuencias del riesgo se reducen trasladando o, de otro modo, compartiendo una parte del riesgo. Adicionalmente puede analizarse si es posible mejorar la efectividad del control asociado al riesgo.

- **Aceptar:** No se emprende ninguna acción que afecte a la probabilidad, las consecuencias del riesgo o la efectividad del control asociado al riesgo (por ejemplo, la relación costo – beneficios no lo justifica).

A continuación, en el **Cuadro N° 12** se presentan algunos ejemplos para las estrategias genéricas de tratamiento del riesgo que se encuentran en la literatura, las que sólo tienen la finalidad de ejemplificar esta materia.

Cuadro Nº 12: Ejemplos de Medidas para Tratar el Riesgo Desde el Punto de la Severidad del Riesgo y de la Exposición al Riesgo

EVITAR	COMPARTIR
○ Prescindir de las actividades de una unidad de negocio, agencia regional o subsidiaria. ○ Suspender la producción de una línea de servicio o producto. ○ Terminar con las actividades de un programa, proyecto o sistema. ○ Decidir no emprender nuevas iniciativas/actividades que podrían dar lugar a riesgos excesivos.	○ Adoptar seguros contra pérdidas inesperadas significativas. ○ Establecer acuerdos con otras organizaciones gubernamentales o privadas. ○ Protegerse contra los riesgos utilizando instrumentos del mercado de capital a largo plazo, cuando se tenga autorización para ello. ○ Externalizar procesos de negocio riesgosos siempre que no correspondan al ejercicio mismo de sus facultades. ○ Distribuir el riesgo mediante acuerdos contractuales con entidades que actúen como clientes, proveedores u otros interesados.
REDUCIR	**ACEPTAR**
○ Diversificar las ofertas de servicios y productos. ○ Establecer límites en la ejecución del presupuesto por región o unidad. ○ Establecer procesos de negocio eficaces. ○ Aumentar la implicación de la dirección en la toma de decisiones y el seguimiento. ○ Reasignar los recursos presupuestarios entre las unidades operativas.	○ Provisionar las posibles pérdidas. ○ Confiar en las compensaciones naturales existentes dentro de una cartera. ○ Aceptar el riesgo si se adapta al nivel máximo preestablecido.

3.3. Evaluar y Seleccionar las Estrategias de Tratamiento de los Riesgos

Una vez conocidas las estrategias genéricas para tratar los riesgos, es necesario a través de la evaluación de los costos y beneficios potenciales, determinar qué estrategia va a utilizar la organización gubernamental y hacia dónde orientarlas. Para ello, es necesario tener presente algunas consideraciones:

- Las opciones pueden ser evaluadas sobre la base del grado de reducción de la Severidad del Riesgo (impacto y/o probabilidades), y las mejoras en la efectividad de los controles.

- Deben considerarse una cantidad de opciones individualmente o combinadas. Es posible que una estrategia de respuesta afecte a múltiples riesgos.

- El costo de administrar un riesgo necesariamente debe ser compensado con beneficios relacionados, sean sociales y/o económicos.

- Considerar que los requerimientos legales podrían estar por sobre los resultados del análisis costo-beneficio antes referido.

- Se debe tener en cuenta que un tratamiento al riesgo mediante una estrategia podría introducir nuevos riesgos. Estos también deben identificarse y tratarse adecuadamente.

- El objetivo principal de la selección de las estrategias siempre debe ser el reducir la severidad del riesgo y/o aumentar la efectividad del control existente, acciones que finalmente repercuten en bajar el nivel de la exposición al riesgo.

En el **Cuadro Nº 13** se presenta una relación comparativa de la aplicación de las estrategias y su efecto potencial en la severidad del riesgo y en la efectividad del control.

Cuadro Nº 13: Relaciones Generales Entre las Estrategias y su Efecto en el Riesgo y Efectividad del Control

Estrategias Genéricas	Efecto potencial en los componentes de la Severidad del Riesgo	Efecto potencial en la Efectividad del Control	Situación esperada en relación con el Nivel de Exposición al Riesgo
Evitar	La probabilidad e impacto no se reducen.	-	El Nivel de Exposición al Riesgo está fuera de los límites aceptados por la organización. No se ve afectada.
Reducir	El nivel de probabilidad o impacto se reducen (o ambos).	Mejora su efectividad	El Nivel de Exposición al Riesgo disminuye.
Compartir	El nivel de probabilidad o impacto se reducen (o ambos).	Mejora su efectividad	El Nivel de Exposición al Riesgo disminuye.
Aceptar	La probabilidad e impacto no se reducen.	-	El Nivel de Exposición al Riesgo debiera estar ya dentro de los límites con que la organización puede aceptar operar.

3.4. Preparar e Implementar Planes de Tratamiento y Monitoreo

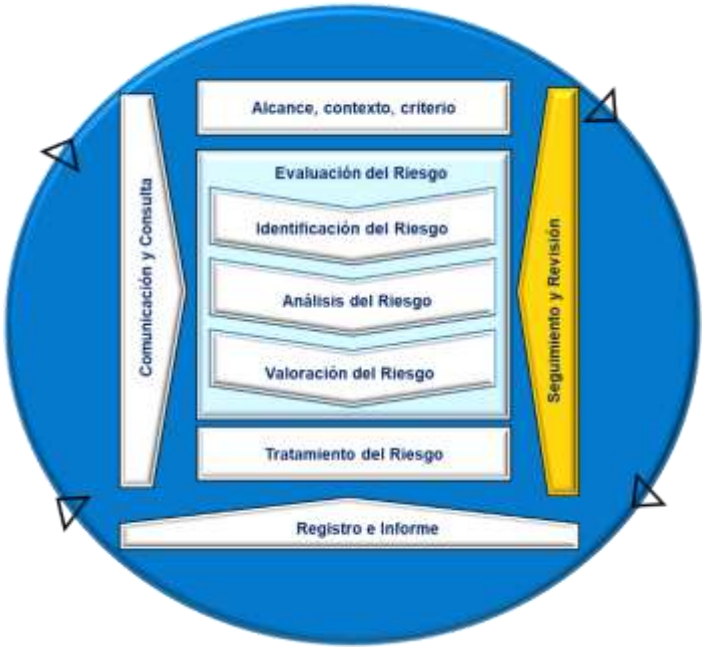
La dirección de la organización gubernamental debe aprobar los planes y estrategias seleccionadas. En consideración a que, dentro de los procesos y subprocesos priorizados, deben tratarse todos los riesgos que corresponden a las actividades de las etapas que éstos últimos contienen, así como los riesgos de entrada y salida de cada subproceso, es recomendable gestionar los riesgos bajo una perspectiva de cartera o portafolio, esto implica analizar los riesgos en su conjunto, considerando cómo los riesgos individuales se interrelacionan en el ámbito organizacional.

Debe definirse responsables de la estrategia, plazos, indicadores de logro, periodo de medición, etc.

4. Fase: Seguimiento y Revisión

La fase de seguimiento y revisión tiene como finalidad asegurar que el sistema y el proceso de gestión de riesgos mantengan su eficacia, consistencia y alineación con el contexto institucional, permitiendo que se adapten adecuadamente a los cambios en el contexto estratégico, operativo o normativo de la entidad.

Figura N° 12: Fase Seguimiento y Revisión



Fuente: NCh-ISO 31000:2018 – INN

Esta fase contempla la evaluación sistemática del desempeño de los tratamientos de riesgos implementados, así como la efectividad y suficiencia de los controles existentes, asegurando que los riesgos se mantengan dentro de los niveles aceptables definidos por la organización.

El seguimiento y revisión permite identificar desviaciones, oportunidades de mejora, riesgos emergentes o modificaciones en la exposición institucional, habilitando ajustes oportunos y decisiones informadas.

Las fuentes que permitirán efectuar esta revisión periódica son las siguientes:

- Resultados de auditorías internas o externas.
- Indicadores de desempeño (KRI u otros).
- Reclamos o alertas ciudadanas.
- Evaluaciones de cumplimiento.
- Cambios normativos, presupuestarios o estratégicos.

En conjunto, esta fase constituye un mecanismo de retroalimentación continua, indispensable para el fortalecimiento progresivo y dinámico del sistema de gestión de riesgos.

La responsabilidad del monitoreo recae en diversos actores institucionales, quienes deben velar por la efectividad de todos los pasos del Proceso de Gestión de Riesgos, para asegurar que se está cumpliendo adecuadamente y que las circunstancias cambiantes no alteran las prioridades al afectar las ponderaciones estratégicas, las probabilidades o impactos de los riesgos, etc. Son las siguientes:

- Unidades gestoras del riesgo deben realizar el seguimiento directo.
- Unidad o encargado de riesgos institucional coordina la revisión global.
- Comité de Riesgos (si existe) valida los resultados y propone ajustes estratégicos.
- Unidad de Auditoría Interna puede contribuir con evaluaciones independientes y recomendaciones.

Por su parte, la organización gubernamental debe establecer formalmente responsables del monitoreo y formular estructuras de reportes útiles a la organización, que le permita a la dirección, obtener información relevante, en forma oportuna y periódica sobre el estado de los riesgos en cualquier etapa del proceso.

Asimismo, se recomienda fomentar en la cultura organizacional la práctica de modelos de autoevaluación sistemática de riesgos, como instrumento de fortalecimiento del control interno, aprendizaje institucional y madurez del sistema de gestión.

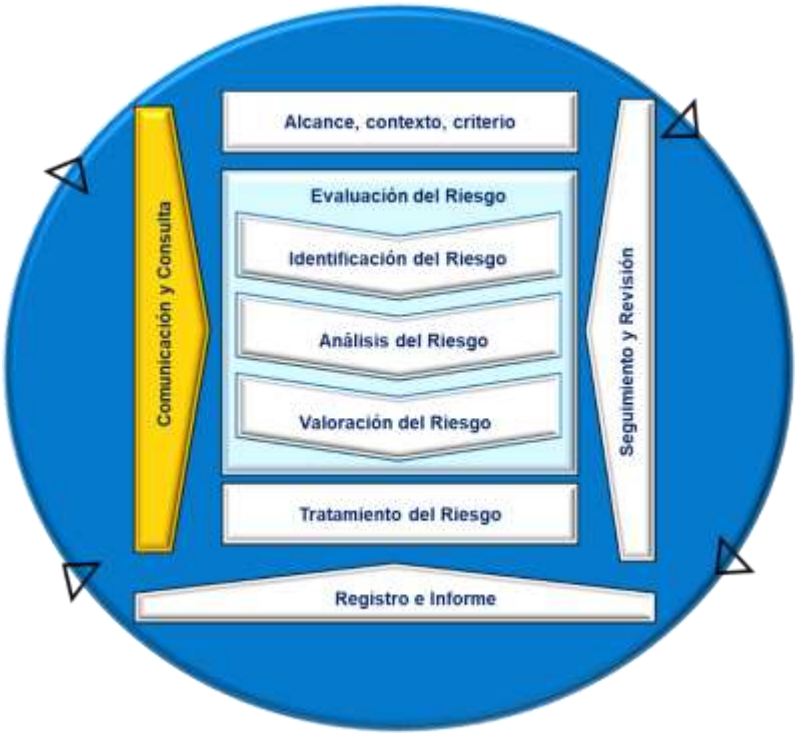
Actividades Recomendadas para Monitorear los Planes de Tratamiento y Monitoreo

- Seguimiento de las estrategias seleccionadas y monitoreo de las actividades requeridas.
- Verificar periódicamente el avance en la implementación de la estrategia de tratamiento de los riesgos.
- También se deben analizar y evaluar los controles existentes que contribuyen a asegurar el cumplimiento de las medidas tomadas para mitigar los riesgos.
- La auditoría interna tiene un rol fundamental en esta actividad, los planes de auditoría deben considerar la evaluación de las actividades de monitoreo y el seguimiento de la implantación de las estrategias de tratamiento de los riesgos.

5. Fase: Comunicación y Consulta

La comunicación y la consulta constituyen un elemento transversal y continuo en todas las fases del Proceso de Gestión de Riesgos. Su propósito es asegurar que las partes interesadas, tanto internas como externas, estén debidamente informadas, puedan participar cuando corresponda, y comprendan las decisiones y fundamentos asociados a la identificación, análisis, valoración, tratamiento, seguimiento y mejora de los riesgos institucionales.

Figura N° 13: Fase Comunicación y Consulta



Fuente: NCh-ISO 31000:2018 – INN

Si bien esta fase se explica metodológicamente en este punto, en la práctica, debe desarrollarse desde el inicio de la implantación del proceso y mantenerse activa durante toda su ejecución y actualización.

5.1. Plan de Comunicación y Consulta

Se debe elaborar y mantener un Plan de Comunicación y Consulta, adaptado a la realidad y estructura organizacional, que asegure la circulación eficaz de la información y la participación adecuada de los actores clave.

Componentes mínimos sugeridos:

- Identificación de usuarios internos y externos, su rol y relevancia respecto al proceso.
- Tipo de información a remitir y recibir en cada fase.
- Asignación de responsabilidades respecto de la generación, validación y control de calidad de la información.
- Periodicidad para el envío y actualización de la información.
- Definición de canales, soportes y sistemas utilizados para gestionar la información.
- Especificación de reportes, incluyendo contenido, análisis e indicadores clave.
- Procedimientos de comunicación, acceso y seguridad de la información.
- Criterios de participación y retroalimentación, incluyendo mecanismos para recolección y análisis de opiniones.

Para facilitar la aplicación práctica de esta fase, se adjunta el **Anexo Nº 17** – Ejemplo de un Plan de Comunicación y Consulta, el cual proporciona una estructura sugerida que puede ser adaptada por cada entidad según su realidad organizacional, nivel de madurez y contexto institucional.

5.2. Implementación y Revisión del Plan

El plan debe ser implementado en paralelo con el proceso de gestión de riesgos y evaluado periódicamente. Algunas preguntas guía para esta evaluación incluyen:

- ¿La información contiene todos los elementos necesarios?
- ¿Se entrega de manera oportuna y actualizada?
- ¿Es precisa, completa y accesible para quienes la necesitan?
- ¿Facilita la toma de decisiones informadas?

Además, se debe procurar el uso de tecnologías de información e interoperabilidad, que permitan integrar sistemas internos y externos, y obtener datos actualizados en línea.

5.3. Roles y Responsabilidades en el Plan

- El Jefe de Servicio es el responsable final del proceso, incluyendo la comunicación y consulta.
- Los Directivos responsables de procesos deben asegurar que la información de su área sea precisa y oportuna.
- Todo el personal de la entidad tiene responsabilidad en el cumplimiento y participación.
- La Unidad de Auditoría Interna debe apoyar a la autoridad en la coordinación, monitoreo y mejora del proceso, sin perjuicio de sus funciones de aseguramiento.

5.4. Componente: Temas Relativos al Riesgo

Entre los antecedentes que se pueden considerar están:

- Reportes de análisis de indicadores relacionados con el Proceso de Gestión de Riesgos en general.
- Reportes de análisis relacionados con la Matriz de Riesgos Estratégica al Jefe de Servicio y responsables de las áreas en la organización.
- Reportes de actualización del análisis de riesgos.
- Reportes del Plan de Tratamiento de Riesgos al Jefe de Servicio y responsables de las áreas en la organización.

Algunos ejemplos de criterios e indicadores (la organización gubernamental debe diseñar sus propios indicadores de acuerdo con su naturaleza y necesidades) que pueden establecerse en relación con el análisis de la información derivada del Proceso de Gestión de Riesgos, se muestran a continuación en el **Cuadro Nº 14**.

Sin perjuicio de la periodicidad en que el Jefe de Servicio y el CAIGG requiera el envío de los resultados de los indicadores y en general de los distintos reportes, la organización debería definir responsables y plazos para monitorear los cambios de estos resultados y así obtener información oportuna que ayude a la toma de decisiones de la Dirección.

Cuadro Nº 14: Ejemplos de Criterios e Indicadores para Análisis de Información del Proceso de Gestión de Riesgos

Criterio	Posibles Indicadores para Análisis (La lista no es taxativa)	Responsable	Plazos
Asociados a Comprensión del Proceso de Gestión de Riesgos			
Calidad Cursos y Talleres	• Áreas con mayor cantidad de participantes. • Materias de mayor complejidad para los alumnos. • Áreas de mejor rendimiento en el curso.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Nivel de Aplicación	• Áreas que mejor desarrollan el Proceso. • % de personas involucradas por área.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Asociados a los Reportes del Proceso de Gestión de Riesgos			
Oportunidad Reportes	• Cumplimiento con la distribución del reporte. • Días de retraso respecto del Plan de comunicación.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Calidad Contenido	• Exactitud de la información del reporte. • Completitud de análisis del reporte. • Nivel de medidas correctivas y preventivas comprometidas en reporte de tratamiento.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Asociados a la Matriz de Riesgos Estratégica del Proceso de Gestión de Riesgos			
Severidad del Riesgo	• Procesos con más altas severidades del riesgo. • Subprocesos con más altas severidades de riesgo. • Etapas con más altas severidades de riesgo.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Exposición al Riesgo	• Procesos con más altas exposiciones al riesgo. • Subprocesos con más altas exposiciones al riesgo. • Etapas con más altas exposiciones al riesgo.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En los meses de enero y octubre de cada año.
Impacto al Riesgo	• Procesos con riesgos de impactos más altos. • Subprocesos con riesgos de impactos más altos. • Etapas con riesgos de impactos más altos.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Tipos de Riesgos	• Tipologías de Riesgos que más se repiten. • Tipos de riesgos con mayor exposición. • Tipos de riesgos con mayor impacto.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.

Criterio	Posibles Indicadores para Análisis (La lista no es taxativa)	Responsable	Plazos
Controles	• Procesos con controles más efectivos. • Procesos con controles menos efectivos. • Riesgos extremos con controles menos efectivos.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Ranking	• Procesos en los primeros lugares del ranking y su relación al negocio. • Procesos en los primeros lugares del ranking y su relación al soporte. • Procesos priorizados y profundidad del levantamiento realizado.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Asociados a Otras Dimensiones del Proceso de Gestión de Riesgos			
....	....	....	....

5.5. Componente: Realizar Comunicaciones y Consultas Internas y Externas Eficaces

El objetivo es asegurarse que los responsables de la implementación del Proceso de Gestión del Riesgo y las partes interesadas en la organización comprenden las bases que han servido para tomar decisiones y las razones por las que son necesarias determinadas acciones. Entre los antecedentes que se pueden considerar están los siguientes:

- Identificar usuarios o clientes internos y externos, y su nivel e importancia para el Proceso de Gestión de Riesgos.
- Definir qué tipo de información se espera recibir y remitir en el proceso.
- Definir roles y responsables de la calidad y confiabilidad para la información a recibir y remitir.
- Definir periodicidad para la información a recibir y remitir.
- Identificar y definir sistemas, canales y mecanismos para manejar la información de gestión de riesgos al interior de la organización y para remitirla externamente.
- Definir qué tipo de reportes tendrá el proceso. Definir Tipo de análisis que se incluirán en los reportes.
- Definir el procedimiento de cómo se realizará la comunicación, identificar los soportes y tecnologías requeridas.
- Definir cómo y quiénes tendrán acceso a la comunicación, señalar los criterios para definir perfiles por tipo de información.
- Definir cómo se recolectarán opiniones que genere la comunicación, espacios de participación, forma como se hará efectiva la participación.

Posteriormente, se debería analizar, a una fecha dada, los resultados de la aplicación de los “Planes de Comunicación y Consulta” y emitir un informe. Solicitar a los usuarios de la información contestar algunas de las siguientes preguntas relacionadas con el contenido, oportunidad, actualidad, exactitud y accesibilidad de los reportes internos y externos, puede ser de utilidad para esta tarea. Entre otros se pueden considerar las siguientes:

- En relación con el contenido. ¿Contiene toda la información necesaria?
- En relación con la oportunidad. ¿Se facilita en el tiempo adecuado?
- En lo relativo a la actualidad. ¿Es la información más reciente disponible?
- En relación con la exactitud. ¿Los datos son correctos?
- En relación con la completitud. ¿Los datos son completos?
- Por último, en relación con la accesibilidad. ¿Puede ser obtenida fácilmente por las personas adecuadas?

Debe propenderse a mejorar la calidad de la información, incorporándose las tecnologías de información que le permitan interoperar entre distintos sistemas y plataformas, en forma interna y externa, obteniendo datos en línea de las actividades del negocio y en particular del Proceso de Gestión de Riesgos.

Es importante reiterar que el desarrollo de cada una de las fases del Proceso de Gestión de Riesgos es en primer lugar responsabilidad del Jefe de Servicio de la entidad y luego también es responsabilidad de todos los ejecutivos responsables de cada proceso y finalmente de todo el personal. La auditoría interna por su parte debe apoyar a la referida autoridad a coordinar la mantención y mejoramiento del proceso y a monitorear su adecuado avance en las diferentes fases, sin perjuicio de las actividades de aseguramiento contempladas en el Plan Anual de Auditoría aprobado por la dirección.

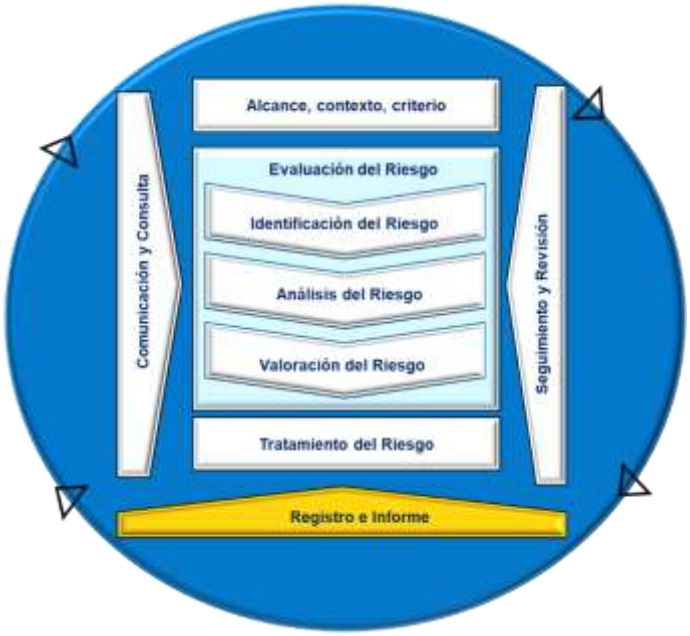
6. Fase: Registro e Informe

El registro e informe constituyen una fase clave del Proceso de Gestión de Riesgos, cuya finalidad es asegurar la trazabilidad, transparencia y rendición de cuentas respecto de las decisiones adoptadas, actividades ejecutadas y resultados obtenidos a lo largo del proceso.

Según la norma NCh-ISO 31000:2018, esta fase debe contribuir a:

- Comunicar eficazmente las actividades y resultados del proceso.
- Proporcionar información útil para la toma de decisiones.
- Apoyar la mejora continua del sistema de gestión de riesgos.
- Facilitar la interacción con las partes interesadas, especialmente con aquellas con responsabilidades de supervisión y control.

Figura N° 14: Fase Registro e Informe



Fuente: NCh-ISO 31000:2018 – INN

6.1. Contenidos Mínimos del Registro

Los registros generados durante la gestión de riesgos deben ser suficientes para:

- Reconstruir las decisiones y supuestos considerados en cada fase.
- Evaluar la consistencia metodológica del proceso.
- Extraer lecciones aprendidas y oportunidades de mejora.
- Demostrar cumplimiento con las responsabilidades institucionales, normativas y de control.

Entre los elementos a registrar se consideran:

- Versiones de la matriz de riesgos institucional.
- Actas y/o respaldos de talleres o reuniones técnicas.
- Informes de análisis, valoración y tratamiento de riesgos.
- Seguimiento de planes de acción y controles asociados.
- Informes periódicos o extraordinarios remitidos a instancias directivas o externas (ej. CAIGG, órganos de control).
- Documentación de revisiones, auditorías, autoevaluaciones o retroalimentaciones recibidas.

6.2. Criterios para la Gestión Documental

Las decisiones sobre qué, cómo y dónde registrar la información deben considerar al menos los siguientes criterios:

- Las necesidades de aprendizaje organizacional continuo.
- El valor de la reutilización de información para mejorar el proceso.
- El costo y esfuerzo asociado a crear y mantener los registros.

- Los requerimientos legales, reglamentarios y operacionales.
- Los mecanismos de acceso, búsqueda y recuperación eficiente.
- Los plazos de conservación aplicables a la documentación.
- El nivel de sensibilidad y seguridad de la información contenida.

6.3. Informes de Gestión del Riesgo

El proceso debe generar reportes regulares y estructurados que respondan a las necesidades de:

- Alta Dirección y jefaturas de proceso.
- Función de Auditoría Interna.
- Comité de Riesgos (si existe).
- Autoridades externas (ej. CAIGG, organismos fiscalizadores).
- Otras partes interesadas pertinentes, según el contexto.

Factores a considerar en los informes:

- Público objetivo: necesidades y requerimientos de cada actor.
- Frecuencia y oportunidad: mensual, trimestral, semestral o según hitos.
- Método de presentación: digital, verbal, escrito, mediante dashboards u otros.
- Relevancia del contenido: alineación con objetivos estratégicos, resultados clave, incidentes críticos y decisiones requeridas.

6.4. Rol Estratégico del Registro e Informe

Esta fase es parte integral de la gobernanza institucional, y no debe limitarse a una función administrativa. Una gestión adecuada de la información generada permite:

- Elevar la calidad del diálogo interno y externo sobre riesgos.
- Apoyar a la alta dirección en sus funciones de conducción estratégica.
- Proveer evidencia ante instancias de control, fiscalización o auditoría.
- Integrar el proceso de riesgos con otros sistemas institucionales (ej. planificación, control interno, cumplimiento normativo, CAIGG).

VI. GESTIÓN DE RIESGOS DE PROBIDAD ADMINISTRATIVA

1. Introducción

La gestión de riesgos de probidad administrativa se fundamenta en el deber constitucional y legal de observar el principio de probidad en el ejercicio de la función pública, entendido como la obligación de desarrollar una conducta funcionaria intachable y un desempeño honesto y leal de la función o cargo, con preeminencia del interés general sobre el particular, conforme al artículo 8° de la Constitución Política de la República y a la Ley N° 18.575.

Este deber no se limita a la reacción frente a infracciones consumadas, sino que impone una exigencia estructural de prevención, diseño adecuado de controles, gestión activa de conflictos de interés y ejercicio efectivo del deber de supervisión jerárquica.

El debilitamiento de la probidad administrativa expone a las instituciones públicas a riesgos críticos, tales como:

- Perjuicios patrimoniales.
- Afectación reputacional.
- Pérdida de confianza ciudadana.
- Debilitamiento de la legitimidad institucional.
- Sanciones administrativas.

En consecuencia, la gestión de riesgos de probidad constituye un componente especializado del sistema de control interno y del proceso institucional de gestión de riesgos, alineado entre otras regulaciones con:

- Ley N° 18.575 (Bases Generales de la Administración del Estado).
- Ley N° 20.880 (Conflictos de Interés y DIP).
- Ley N° 19.886 (Contratación Pública).
- Ley N° 10.336 (CGR).
- Ley N° 18.834 (Estatuto Administrativo).
- Ley N° 21.634, Capítulo VII (Compras Públicas)
- Ley N° 19.653 (Sobre Probidad Administrativa)
- Estándares internacionales emitidos por INTOSAI, así como marcos de referencia como la norma ISO 31000 sobre gestión de riesgos, ISO 37001 sobre sistemas de gestión antisoborno y el marco COSO ERM (*Enterprise Risk Management*) sobre gestión de riesgos corporativos.

La experiencia jurisprudencial administrativa ha reforzado el carácter preventivo y objetivo del principio de probidad, estableciendo que la omisión del deber de control y la persistencia de vulnerabilidades conocidas constituyen factores agravantes de responsabilidad.

Los estándares metodológicos y criterios establecidos en el presente capítulo tienen carácter orientador y preliminar, en cuanto responden al estado actual del marco normativo, jurisprudencial y de mejores prácticas en materia de probidad administrativa. No obstante, la naturaleza dinámica de los riesgos de probidad, caracterizados por su capacidad de adaptación, mutación y sofisticación, exige que esta herramienta sea objeto de revisión, actualización y mejora continua. En consecuencia, los servicios públicos deberán entender este marco como un instrumento evolutivo, susceptible de ajustes periódicos conforme a cambios regulatorios, tecnológicos, organizacionales o a nuevas tipologías de riesgo emergente.

Finalmente, en atención a la naturaleza jurídica, materialidad institucional y especial criticidad de los riesgos de probidad administrativa, los servicios públicos deberán elaborar y mantener una **Matriz de Riesgos de Probidad Administrativa** diferenciada y autónoma respecto de la Matriz de Riesgos Estratégicos institucional. Esta separación no es meramente formal, sino que responde a la necesidad de asegurar un análisis específico, exhaustivo y técnicamente focalizado en riesgos que comprometen directamente el principio de probidad. La integración posterior con la matriz estratégica podrá realizarse a efectos de consolidación o reporte, pero en ningún caso sustituirá la obligación de contar con una matriz especializada que permita identificar, evaluar, tratar y monitorear los riesgos de probidad con criterios propios, trazabilidad diferenciada y supervisión reforzada.

El formato de la Matriz de Riesgos de Probidad Administrativa será disponibilizada por el CAIGG en la respectiva página web, y actualizados anualmente.

2. Alcance

La gestión de riesgos de probidad administrativa será aplicable a todos los órganos de la Administración del Estado y comprenderá la totalidad de sus procesos estratégicos, operativos, de apoyo y transversales.

Se deberá prestar especial atención a aquellos procesos que:

- Involucren toma de decisiones con discrecionalidad administrativa.
- Supongan interacción con terceros, proveedores, beneficiarios o usuarios.
- Administren o gestionen recursos públicos financieros, humanos o materiales.
- Presenten antecedentes históricos de observaciones, sanciones o debilidades estructurales de control.

Los riesgos de probidad deberán incorporarse de manera transversal en el Proceso de Gestión de Riesgos institucional, asegurando trazabilidad entre:

Criterio normativo → Vulnerabilidad → Riesgo → Tipo de control → Evidencia → Riesgo residual → Decisión de gobernanza.

3. Definiciones para Gestión de Riesgos de Probidad

Para efectos de este capítulo, se considerarán, entre otras, las siguientes definiciones específicas:

Probidad administrativa: Deber de observar conducta funcionaria intachable y desempeño honesto y leal con preeminencia del interés general, conforme a la Constitución y Ley N° 18.575.

Conflicto de interés: Situación en que el interés personal, familiar o económico de una autoridad o funcionario puede influir, o parecer influir, en el ejercicio imparcial de sus funciones, conforme a la Ley N° 20.880 y su reglamento.

Riesgo de probidad: Posibilidad de que, por acción u omisión, se vulneren deberes de probidad administrativa, afectando legalidad, imparcialidad, transparencia, correcto uso de recursos públicos o confianza institucional, aun cuando no exista perjuicio patrimonial directo.
Señales de alerta / banderas rojas: Hechos, patrones o condiciones anómalas que justifican revisión ampliada o escalamiento, tales como concentración de decisiones, excepciones reiteradas, falta de trazabilidad o inacción frente a advertencias previas.

Las demás definiciones generales sobre riesgo, causa, consecuencia, vulnerabilidad y controles serán las establecidas en el marco metodológico general del presente Documento Técnico.

4. Metodología para la Identificación y Gestión de los Riesgos de Probidad Administrativa

La gestión de riesgos de probidad administrativa deberá desarrollarse conforme a las fases del Proceso de Gestión de Riesgos institucional, integrando criterios específicos derivados del principio de probidad consagrado en el artículo 8° de la Constitución y en la Ley N° 18.575.

Su aplicación debe ser coherente principalmente con:

- El deber de control jerárquico.
- Las obligaciones de prevención de conflictos de interés (Ley N° 20.880).
- Norma sobre gestión institucional del riesgo (ISO 31000).
- Norma sobre sistemas de gestión antisoborno (ISO 37001).
- El marco de gestión de riesgos Corporativo (COSO ERM).

La identificación de riesgos de probidad deberá iniciar con un análisis estructurado del contexto, considerando al menos:

4.1. Contexto Externo

- Marco legal y regulatorio aplicable.
- Jurisprudencia administrativa vigente.
- Nivel de escrutinio público.
- Relaciones contractuales o regulatorias con terceros.
- Entorno político-administrativo.

Este análisis permite determinar estándares reforzados de diligencia en procesos con mayor exposición reputacional o patrimonial.

4.2. Contexto Interno

- Estructura organizacional.
- Cultura ética institucional.
- Liderazgo y “tone at the top”
- Roles y responsabilidades formalmente definidos.
- Sistemas de control interno existentes.
- Historial de observaciones de auditoría o dictámenes de control.

La jurisprudencia administrativa ha establecido que la ausencia de supervisión efectiva puede configurar incumplimiento del deber de control, aun cuando no exista beneficio personal directo.

4.3. Contexto del Proceso

Para cada proceso crítico deberá identificarse:

- Objetivo institucional del proceso.
- Etapas críticas.
- Puntos de decisión.

- Nivel de discrecionalidad.
- Interacciones con recursos públicos.
- Interacciones con terceros.

Sin delimitación clara del contexto no es posible identificar adecuadamente el riesgo de probidad.

4.4. Identificación de Vulnerabilidades Asociadas a la Probidad

Las organizaciones deberán identificar vulnerabilidades estructurales que puedan facilitar la materialización de riesgos de probidad administrativa.

Entre ellas:

- Concentración de funciones en una misma persona.
- Insuficiente segregación de funciones.
- Falta de revisión independiente.
- Débil supervisión jerárquica.
- Ambigüedad normativa o procedimental.
- Falta de trazabilidad documental.
- Persistencia de observaciones no corregidas.
- Controles meramente formales sin evidencia operativa.

Criterio Técnico Reforzado

La persistencia de vulnerabilidades conocidas constituye un factor agravante en materia de responsabilidad administrativa y debe incrementar la probabilidad estimada del riesgo.

La reiteración de observaciones no subsanadas es un indicador directo de riesgo de probidad, aun cuando no exista sanción formal.

4.5. Identificación de Riesgos de Probidad Administrativa

Los riesgos deberán formularse de manera clara, vinculados al objetivo del proceso, considerando tanto acciones como omisiones.

Se recomienda estructurar el riesgo en la siguiente lógica:

Evento (acción u omisión)

- Vulnerabilidad estructural
- Consecuencia institucional

Ejemplo:

“Riesgo de adopción de decisiones discrecionales sin ejercicio del deber de abstención, producto de ausencia de protocolos formales de conflicto de interés, afectando imparcialidad y legitimidad institucional.”

No es necesario acreditar perjuicio patrimonial para configurar un riesgo de probidad; basta la afectación potencial a la imparcialidad o confianza pública.

5. Técnicas para la Identificación de Riesgos de Probidad Administrativa

Con el objeto de asegurar una identificación sistemática, homogénea y jurídicamente consistente de los riesgos de probidad administrativa, deberán aplicarse técnicas que permitan distinguir claramente:

- Riesgos de gestión ordinaria.
- Riesgos que comprometen el principio de probidad.
- Vulneraciones potenciales al deber de control.

Las técnicas descritas a continuación son complementarias y deberán aplicarse de manera proporcional al nivel de exposición institucional.

5.1. Técnica: Análisis Estructurado de Configuración del Riesgo de Probidad Administrativa

Todo riesgo de gestión identificado deberá analizarse a la luz de los elementos que permiten determinar si puede configurarse como riesgo de probidad administrativa.

Para ello, se utilizará una matriz estructurada que considere, al menos, los siguientes componentes:

Elementos de Evaluación

1. **Descripción del riesgo**
   - Riesgo formulado en relación con el objetivo del proceso.
2. **Acción u omisión**
   - Conducta activa o pasiva que pueda vulnerar el deber de probidad.
   - Se incluye omisión del deber de control jerárquico.
3. **Uso del poder o posición funcionaria**
   - Existencia de atribuciones, discrecionalidad o influencia derivada del cargo.
4. **Desviación de la gestión de lo público**
   - Afectación a la legalidad, imparcialidad, finalidad pública o correcta administración de recursos.
5. **Beneficio privado o ventaja indebida**
   - Real o potencial, patrimonial o no patrimonial.
6. **Configuración como riesgo de probidad**
   - Evaluación integrada de los elementos anteriores.

Criterio metodológico

No es indispensable la concurrencia copulativa de todos los elementos para configurar un riesgo de probidad.

Basta la afectación potencial a la imparcialidad, legalidad o deber de resguardo del interés general para calificarlo como tal.

Esta matriz es una herramienta preventiva de análisis estructural, no un instrumento sancionatorio.

Cuadro Nº 15: Estructura para la Definición de Riesgos de Probidad Administrativa

MATRIZ: DEFINICIÓN DE RIESGO DE PROBIDAD ADMINISTRATIVA						
Descripción del Riesgo (1)	**Acción u Omisión (2)**	**Uso del poder (3)**	**Desviar la gestión de lo público (4)**	**Beneficio privado (5)**	**Configuración como Riesgo de Probidad (6)**	**Conclusión**
Riesgo 1						
Riesgo 2						
Riesgo n						

Instrucciones de uso

- Marcar con “X” cuando el elemento esté presente.
- Justificar brevemente en la columna “Conclusión”.
- Documentar criterio normativo aplicable.

(1) **Identificación del Riesgo de Gestión:** Describir el riesgo de gestión específico previamente identificado en la matriz de riesgos institucional, indicando el proceso o actividad afectada.

(2) **Evaluación de Acción u Omisión:** Este elemento analiza si el riesgo de gestión implica la realización de una acción indebida o la omisión de una actuación exigida por el marco normativo o procedimental, que pueda afectar el cumplimiento del principio de probidad administrativa.
Importancia: La acción u omisión constituye un elemento central en la configuración de riesgos de probidad administrativa, especialmente considerando que la jurisprudencia ha reconocido la responsabilidad por omisión del deber de diligencia, supervisión o control.
Acción a ejecutar: Analizar si el riesgo involucra una acción u omisión relevante desde la perspectiva de la probidad administrativa. En caso afirmativo, indicar brevemente el tipo de acción u omisión identificada y/o marcar con una “X”.

(3) **Uso del Poder o de la Posición Funcionaria:** Se refiere a la utilización, aprovechamiento o influencia derivada de la posición funcionaria, atribuciones, jerarquía o grado de discrecionalidad para incidir en decisiones, actuaciones o procesos administrativos.
Importancia: El uso del poder o de la posición funcionaria es un factor relevante en riesgos de probidad administrativa, aunque no es un requisito indispensable, ya que estos riesgos pueden configurarse también en niveles operativos o mediante omisiones.
Acción a ejecutar: Determinar si el riesgo identificado implica el uso, abuso o aprovechamiento de facultades, atribuciones o influencia funcionaria. De corresponder, señalar el elemento afectado y/o marcar con una “X”.

(4) **Desviación de la Gestión de lo Público:** Este elemento evalúa si el riesgo puede provocar una afectación a la finalidad pública, la legalidad, la imparcialidad o la correcta administración de los recursos y procesos públicos.

Importancia: La desviación de la gestión pública es un indicador relevante de riesgo de probidad administrativa, especialmente cuando se afecta la confianza pública, aun cuando no exista perjuicio patrimonial directo.
Acción a ejecutar: Evaluar si el riesgo implica desviar, distorsionar o afectar la gestión adecuada de recursos, procesos o decisiones públicas. En caso afirmativo, describir brevemente el efecto identificado y/o marcar con una "X".

(5) **Beneficio Privado o Ventaja Indebida:** Corresponde a la existencia de un beneficio, ventaja o interés particular, directo o indirecto, patrimonial o no patrimonial, para una persona o tercero, derivado de la materialización del riesgo.
Importancia: Si bien el beneficio privado es un elemento relevante, la jurisprudencia administrativa ha establecido que no siempre es necesario acreditar un beneficio económico directo para configurar una infracción al principio de probidad.
Acción a ejecutar: Identificar si el riesgo podría generar un beneficio o ventaja indebida, aun cuando sea potencial, indirecta o no patrimonial. De corresponder, indicar el elemento afectado y/o marcar con una "X".

(6) **Configuración como Riesgo de Probidad Administrativa:** Este elemento corresponde a una evaluación integral de los elementos anteriores, orientada a determinar si el riesgo de gestión analizado puede configurarse como un riesgo de probidad administrativa.
Criterio metodológico clave: Para que un riesgo de gestión se configure como riesgo de probidad administrativa no es necesario que concurran todos los elementos en forma copulativa. La presencia de uno o más elementos relevantes, evaluados en su conjunto y contexto, puede ser suficiente para su calificación.
Acción a ejecutar: Decidir, sobre la base del análisis efectuado, si el riesgo de gestión se configura como un riesgo de probidad administrativa (Sí / No), justificando brevemente la decisión.

Criterios orientadores para la Configuración del Riesgo de Probidad Administrativa

- Todos los elementos presentes

  Conclusión orientativa: Existe una alta probabilidad de configuración de un riesgo de probidad administrativa, al concurrir acción u omisión, uso de la posición funcionaria, desviación de la gestión pública y beneficio privado o ventaja indebida.

- Ausencia de uno o más elementos

  (2) Acción u Omisión ausente
  Implicación: Dificulta la identificación de una conducta relevante desde la probidad administrativa.
  Configuración del riesgo: Poco probable, salvo que existan omisiones estructurales relevantes.

  (3) Uso del poder ausente
  Implicación: El riesgo también puede originarse, especialmente en niveles operativos o por omisión de deberes.
  Configuración del riesgo: Posible, dependiendo del contexto.

  (4) Desviación de la gestión pública ausente

Implicación: Puede no existir afectación directa a recursos o procesos, pero sí a la imparcialidad o confianza pública.
Configuración del riesgo**:** Posible.

(5) Beneficio privado ausente
Implicación: El beneficio puede ser indirecto, no patrimonial o no evidente.
Configuración del riesgo: Posible, especialmente en casos de afectación al deber de imparcialidad.

5.2. Técnica: Análisis de Procesos con Foco en Puntos de Decisión

Se deberán identificar puntos críticos donde exista:

- Discrecionalidad relevante.
- Autorización o validación.
- Priorización de recursos.
- Interacción con terceros.

En cada punto se deberá evaluar:

- ¿Quién decide?
- ¿Con qué nivel de discrecionalidad?
- ¿Con qué controles previos y posteriores?
- ¿Existe trazabilidad documental?
- ¿Qué ocurre si no se ejerce el deber de abstención?

Esta técnica permite detectar riesgos por omisión, especialmente relevantes en jurisprudencia administrativa reciente.

5.3. Técnica: Revisión de Antecedentes Históricos y Jurisprudenciales

Constituyen insumos relevantes y prioritarios, sin carácter taxativo, entre otros los siguientes:

- Dictámenes y pronunciamientos de control.
- Informes de auditoría interna.
- Observaciones reiteradas.
- Sanciones administrativas previas.
- Denuncias fundadas.

La reiteración de observaciones no subsanadas incrementa la probabilidad estimada del riesgo.

5.4. Técnica: Talleres Guiados con Responsables de Procesos

Se recomienda realizar sesiones estructuradas con responsables de procesos críticos, utilizando preguntas tales como:

- ¿Qué decisiones podrían generar cuestionamientos de imparcialidad?
- ¿Dónde existe mayor presión para flexibilizar criterios?
- ¿Qué controles podrían fallar en la práctica?

- ¿Existen zonas de baja trazabilidad?

El enfoque deberá ser preventivo y sistémico, evitando personalización.

5.5. Técnica: Identificación de Señales Tempranas de Alerta

Se considerarán indicadores, sin carácter taxativo, tales como:

- Concentración excesiva de decisiones.
- Excepciones reiteradas.
- Falta de evidencia documental.
- Normalización de prácticas informales.
- Inacción frente a advertencias previas.

Estas señales no constituyen infracción por sí mismas, pero elevan el nivel de exposición al riesgo.

6. Análisis y Evaluación de Riesgos de Probidad Administrativa

Los riesgos de probidad administrativa identificados deberán ser analizados y evaluados conforme a los criterios institucionales de probabilidad e impacto, integrando además consideraciones cualitativas propias de la afectación al valor público.

La evaluación deberá realizarse bajo un enfoque prudente, considerando que en materia de probidad el daño reputacional e institucional puede ser más gravoso que el impacto financiero directo.

6.1. Determinación de la Probabilidad

La probabilidad deberá estimarse mediante un enfoque combinado que considere:

a. Criterio de Frecuencia (Evidencia Histórica y/o Predictiva)

La probabilidad deberá estimarse mediante un enfoque combinado que considere una evaluación integral del riesgo desde tres dimensiones complementarias:

Retrospectiva: análisis de antecedentes históricos y evidencia pasada.

Prospectiva: identificación de factores emergentes o condiciones futuras que puedan favorecer la materialización del riesgo.

Perspectiva: análisis contextual y juicio experto sobre vulnerabilidades estructurales o sistémicas de la institución.

En este análisis se deberán considerar, entre otros elementos, si:

- ¿El evento se ha materializado anteriormente?
- ¿Existen observaciones de auditoría reiteradas?
- ¿Existen sanciones previas?

- ¿Se han detectado denuncias fundadas?

Asimismo, deberán incorporarse elementos de carácter predictivo, tales como:

- ¿Existen debilidades estructurales persistentes en el proceso?
- ¿Se han producido cambios organizacionales recientes que aumenten la exposición?
- ¿Existe alta rotación de personal en funciones críticas?
- ¿El proceso presenta altos niveles de discrecionalidad no regulada?
- ¿Existen presiones externas, metas exigentes o incentivos que puedan inducir conductas indebidas?
- ¿Se han identificado tendencias sectoriales o casos similares en otras instituciones comparables?

La reiteración de observaciones no subsanadas constituye un indicador objetivo de incremento de probabilidad, así como la persistencia de vulnerabilidades conocidas.

b. Criterio de Factibilidad (Condiciones Actuales y Futuras)

Se deberá considerar no sólo las debilidades presentes, sino también factores prospectivos y culturales que puedan favorecer la materialización del riesgo.

Se evaluarán, entre otros aspectos, los siguientes:

Condiciones estructurales

- ¿Existen debilidades estructurales no corregidas?
- ¿Existe discrecionalidad sin contrapesos?
- ¿Hay deficiencias en la segregación de funciones?
- ¿El control es meramente formal?
- ¿Existe cultura de tolerancia a prácticas informales?

Factores prospectivos o de evolución futura

- ¿Se prevén cambios organizacionales que puedan debilitar el control?
- ¿Existen procesos de modernización tecnológica aún no consolidados?
- ¿Se proyectan incrementos significativos en recursos, contratos o volumen operativo?
- ¿Existen reformas normativas que generen períodos de transición o incertidumbre?
- ¿Se anticipan cambios en liderazgos clave o alta rotación en áreas críticas?

Factores culturales y entorno de control (alineado con estándares IIA Global)

- ¿La alta dirección comunica activamente la importancia de la probidad?
- ¿Se percibe coherencia entre el discurso institucional y las prácticas reales?
- ¿Existe tolerancia implícita frente a incumplimientos menores?
- ¿Los funcionarios se sienten seguros para reportar irregularidades?
- ¿Existen incentivos formales o informales que puedan favorecer conductas indebidas?
- ¿La cultura organizacional promueve la rendición de cuentas y la transparencia?

La presencia de debilidades estructurales persistentes, sumadas a factores culturales adversos o escenarios prospectivos de alta exposición, incrementa la factibilidad de ocurrencia del riesgo, aun cuando no existan antecedentes históricos de materialización.

6.2. Determinación del Impacto

El impacto corresponde a la magnitud de las consecuencias institucionales que podría generar la materialización del riesgo.

Tratándose de probidad administrativa, el impacto debe evaluarse de manera integrada considerando:

- Impacto reputacional.
- Impacto institucional.
- Impacto disciplinario.
- Impacto operativo.
- Impacto financiero.
- Impacto en confianza ciudadana.

En materia de probidad no se considera impacto “insignificante”, dado que toda vulneración afecta el principio de legalidad y la legitimidad institucional.

6.3. Instrumento de Valorización de Impacto

Cuadro Nº 16: Valoración de Impactos del Riesgo de Probidad Administrativa

N°	Si el riesgo se materializa, ¿podría…?	RESPUESTA	
		SI	NO
1	Afectar la confianza pública en la institución.		
2	Generar cuestionamientos a la imparcialidad.		
3	Provocar observaciones relevantes de órganos de control.		
4	Dar origen a investigaciones administrativas.		
5	Afectar la credibilidad institucional.		
6	Comprometer la legitimidad de decisiones relevantes.		
7	Interrumpir procesos críticos.		
8	Requerir medidas correctivas extraordinarias.		
9	Derivar en responsabilidades institucionales.		
10	Generar impacto público o mediático negativo.		
	TOTAL	0	0

Teniendo presente las respuestas se establece el nivel de impacto de acuerdo con la siguiente valoración, del **Cuadro N° 17**:

Cuadro Nº 17: Nivel de Impacto del Riesgo de Probidad Administrativa

NIVEL	Impacto	Descripción	Riesgos de Integridad
3	MODERADAS	Si el riesgo de probidad administrativa llegara a materializarse, tendría consecuencias de magnitud moderada, con efectos relevantes pero acotados sobre la entidad y/o el proceso afectado.	4 a 5 respuestas afirmativas
4	MAYORES	Si el riesgo de probidad administrativa llegara a materializarse, tendría consecuencias de alta magnitud, afectando significativamente la gestión institucional, la confianza pública o la legitimidad del actuar administrativo.	6 a 8 respuestas afirmativas
5	CATASTRÓFICAS	Si el riesgo de probidad administrativa llegara a materializarse, tendría consecuencias de carácter crítico o desastroso, con efectos severos sobre la entidad, el proceso y la credibilidad institucional.	9 a 10 respuestas afirmativas

No obstante, aun cuando el número se ubique en el umbral inferior, podrá justificarse un impacto mayor si la afectación compromete gravemente el valor público o el deber de control.

6.4. Severidad del Riesgo

Severidad Base (Inherente):

Severidad = Probabilidad (P) × Impacto (I)

Regla reforzada:

Todo riesgo con impacto catastrófico será considerado, al menos, de severidad ALTA, independientemente de su probabilidad.

6.5. Uso del Mapa de Calor Para Priorización

El mapa de calor deberá construirse combinando:

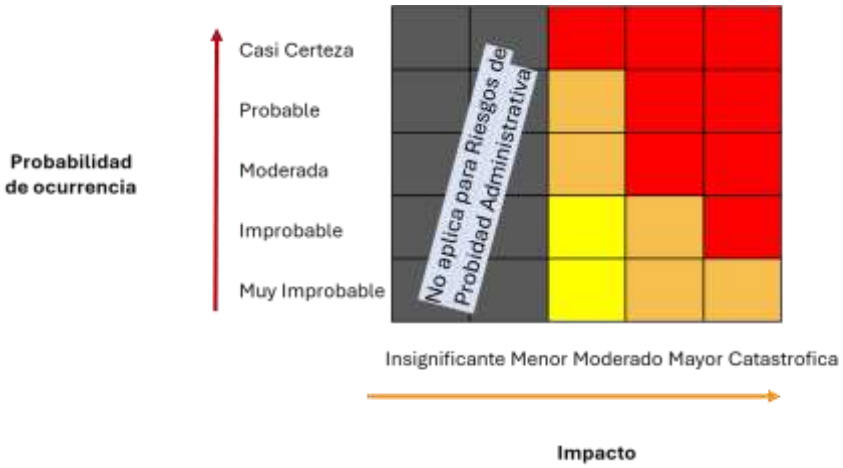
- Nivel de probabilidad.
- Nivel de impacto.
- Ajuste cualitativo cuando corresponda.

Se priorizarán los siguientes escenarios:

- Alta probabilidad + alto impacto.
- Impacto catastrófico aun con baja probabilidad.
- Alta recurrencia estructural.

El mapa de calor deberá excluir riesgos de baja relevancia institucional, concentrando la gestión en zonas críticas (naranjo y rojo).

Figura Nº 15: Mapa de calor para Riesgos de Probidad Administrativa



Este mapa de calor deberá concentrarse, preferentemente, en los siguientes escenarios de riesgo:

- Alta probabilidad y alto impacto, correspondientes a riesgos cuya materialización es altamente probable y cuyas consecuencias afectarían gravemente la gestión, la legitimidad o la confianza pública.
- Alta probabilidad con impacto moderado, cuando la recurrencia del riesgo y la persistencia de sus causas justifican su tratamiento prioritario, aun cuando sus efectos no sean catastróficos de manera individual.
- Impacto catastrófico con probabilidad baja, cuando, aun siendo menos probable, la eventual materialización del riesgo comprometería gravemente la probidad, imparcialidad o legitimidad del actuar institucional.

Este enfoque permite priorizar aquellos riesgos que, de materializarse, podrían afectar de manera significativa la credibilidad institucional, la confianza pública o la sostenibilidad del sistema de control interno.

6.6. Ajuste Cualitativo de Severidad

La severidad base podrá ajustarse mediante evaluación cualitativa de:

- Vulnerabilidad institucional.
- Velocidad de materialización.
- Interdependencia con otros procesos.
- Correlación con otros riesgos.
- Impacto en el valor público.

Severidad Ajustada = Severidad Base × Multiplicador Cualitativo

Este ajuste evita subestimar riesgos que, aun con baja probabilidad, pueden comprometer gravemente la legitimidad institucional.

7. Determinación y uso de la Severidad del Riesgo de Probidad Administrativa

La severidad del riesgo de probidad administrativa constituye el insumo central para la priorización, tratamiento y decisión de gobernanza institucional.

Su determinación no debe interpretarse como un resultado meramente aritmético, sino como una evaluación integrada de criticidad institucional.

7.1. Severidad Base (Riesgo Inherente)

Se calcula conforme a la siguiente fórmula:

Severidad Base = Probabilidad (P) × Impacto (I)

La combinación deberá ubicarse en la matriz institucional de severidad, considerando los siguientes niveles:

- Moderado
- Alto
- Extremo

7.2. Reglas Específicas para Riesgos de Probidad

Tratándose de riesgos de probidad administrativa, se aplicarán las siguientes reglas reforzadas:

- Todo riesgo con impacto Catastrófico será considerado, al menos, de severidad Alta, aun cuando su probabilidad sea baja.
- La reiteración histórica del evento impedirá clasificar el riesgo como moderado.
- La existencia de observaciones no subsanadas incrementará la probabilidad estimada.
- La afectación potencial a la confianza pública podrá justificar elevar la severidad.

7.3. Incorporación al Mapa de Calor de Probidad

La inclusión en el mapa de calor institucional se realizará conforme a las siguientes reglas:

Severidad EXTREMA

- Incorporación obligatoria.
- Requiere acción inmediata.
- Escalamiento a la alta dirección.

- Supervisión reforzada.

Severidad ALTA

- Incorporación obligatoria.
- Plan de tratamiento formal.
- Responsable designado.
- Plazos definidos.

Severidad MODERADA

- Incorporación condicionada.
- Solo si afecta valor público, confianza o legitimidad.

Severidad BAJA

- No se incorpora al mapa de probidad.
- Se gestiona en ámbito general de control interno.

Cuadro Nº 18: Severidad del Riesgo de Probidad Administrativa (Riesgo Inherente)

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)	USO EN MAPA DE CALOR
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)	Siempre visible
Casi Certeza (5)	Mayores (4)	EXTREMO (20)	Siempre visible
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)	Siempre visible
Probable (4)	Catastróficas (5)	EXTREMO (20)	Siempre visible
Probable (4)	Mayores (4)	EXTREMO (16)	Siempre visible
Probable (4)	Moderadas (3)	ALTO (12)	Siempre visible
Moderado (3)	Catastróficas (5)	EXTREMO (15)	Siempre visible
Moderado (3)	Mayores (4)	EXTREMO (12)	Siempre visible
Moderado (3)	Moderadas (3)	ALTO (9)	Siempre visible
Improbable (2)	Catastróficas (5)	EXTREMO (10)	Siempre visible
Improbable (2)	Mayores (4)	ALTO (8)	Siempre visible
Improbable (2)	Moderadas (3)	MODERADO (6)	Condicionado
Muy improbable (1)	Catastróficas (5)	ALTO (5)	Siempre visible
Muy improbable (1)	Mayores (4)	ALTO (4)	Siempre visible
Muy improbable (1)	Moderadas (3)	MODERADO (3)	Condicionado

a. Ajuste de la Severidad del Riesgo

Severidad Base (Inherente)

La severidad base se calcula como:

Severidad Base = Probabilidad (P) × Impacto (I)

Este valor permite una primera clasificación del riesgo (bajo, moderado, alto, extremo).

b. Ajuste Cualitativo de Severidad – Enfoque de Probidad

Para los riesgos de probidad, la severidad base debe ajustarse cualitativamente, reconociendo que el daño al valor público no siempre se refleja plenamente en el cálculo P×I tradicional.

Se incorporan cinco dimensiones cualitativas, entre otras, cada una evaluada en escala 1 (baja) a 3 (alta), con ponderación uniforme. Esta lista no es taxativa, dado que se podrán incorporar otros criterios debidamente justificados.

Cuadro Nº 19: Dimensiones Cualitativas

Variable	Descripción aplicada a probidad
Vulnerabilidad	Grado de exposición de personas, recursos o decisiones críticas.
Velocidad	Rapidez con que el daño se materializa una vez ocurrido el evento.
Interdependencia	Dependencia de otros procesos, actores o sistemas externos.
Correlación	Capacidad del riesgo de activar o potenciar otros riesgos de probidad.
Impacto en el Valor Público	Afectación al mandato, legitimidad y confianza ciudadana.

Cada variable se califica en una escala de 1 (baja), 2 (media), 3 (alta) y se pondera en este caso al 20% del total. La suma ponderada da un multiplicador cualitativo (entre 1.0 y 3.0) que ajusta el riesgo inherente tradicional, tal como se observa en la siguiente tabla.

Cuadro Nº 20: Tabla de Ajuste del Riesgo Inherente

Variable	Valor	Porcentaje Ponderación	Subtotal
Vulnerabilidad	(1 - 3)	20%	V × 0.2
Velocidad	(1 - 3)	20%	VE × 0.2
Interdependencia	(1 - 3)	20%	ID × 0.2

Correlación	(1 - 3)	20%	C × 0.2
Impacto en el Valor Público	(1 - 3)	20%	VP × 0.2
		Total 100%	**Suma= Multiplicador Cualitativo**

Severidad del Riesgo Ajustada= Severidad del Riesgo Tradicional × Multiplicador Cualitativo (M_c)

c. Transición hacia el Tratamiento del Riesgo

Una vez determinada la severidad inherente y ajustada, deberá definirse el tratamiento del riesgo mediante selección de controles adecuados.

Es fundamental distinguir:

- Reducción real de probabilidad (controles preventivos o correctivos estructurales).
- Identificación del evento (controles detectivos).
- Restablecimiento de legalidad (medidas reactivas).

La selección inadecuada del tipo de control puede generar una falsa reducción del riesgo residual.

8. Tratamiento del Riesgo: Clasificación de Controles

La gestión del riesgo deberá considerar la siguiente tipología funcional:

8.1. Controles Preventivos

Reducen probabilidad antes del evento.
Exigencia según severidad:

- Riesgos EXTREMOS: controles preventivos robustos, automatizados o con revisión independiente.
- Riesgos ALTOS: controles preventivos sólidos y documentados.
- Riesgos MODERADOS: controles básicos formalizados.

8.2. Controles Detectivos

Permiten identificar la materialización o señales de alerta.
No reducen por sí mismos la probabilidad futura.

Su eficacia depende de:

- Oportunidad.
- Cobertura.
- Evidencia verificable.

8.3. Medidas Reactivas

Restablecen legalidad y determinan responsabilidades.
No deben considerarse como reducción estructural del riesgo.
Su función es correctiva del evento, no del sistema.

8.4. Controles Correctivos Estructurales

Eliminan causas raíz y reducen probabilidad futura.
Solo cuando:

- Se modifica proceso.
- Se elimina vulnerabilidad.
- Se rediseña arquitectura de control.

Sin análisis de causa raíz no existe reducción real del riesgo.

8.5. Evaluación de la efectividad de los controles

La evaluación de los controles existentes deberá realizarse considerando, al menos, los siguientes criterios:

- Diseño del control: si el control es adecuado para abordar las causas del riesgo.
- Implementación: si el control se encuentra formalmente establecido y en funcionamiento.
- Cobertura: si el control aplica a todas las áreas, procesos o actores relevantes.
- Frecuencia: periodicidad con que el control se ejecuta.
- Responsabilidad: claridad respecto del responsable del control.
- Evidencia: existencia de registros verificables de su aplicación.

Un control que exista solo de manera formal, sin evidencia de aplicación efectiva, no deberá considerarse como un control eficaz para efectos de la gestión del riesgo de probidad.

9. Intensidad del Control según Severidad

Cuadro Nº 21: Intensidad del Control según Severidad

Severidad	Tipo de Control Exigido	Nivel de Supervisión
Extremo	Preventivos reforzados + revisión independiente + detectivos permanentes	Alta Dirección
Alto	Preventivos sólidos + detectivos periódicos	Dirección de Área
Moderado	Preventivos básicos + monitoreo selectivo	Jefatura Directa

Los riesgos de probidad no pueden gestionarse exclusivamente con medidas reactivas.

10. Controles y Deber de Control

En línea con la jurisprudencia administrativa asociada a la materia y a las orientaciones técnicas de la GGSAI N°3, deberá considerarse que la omisión en el ejercicio del deber de control constituye un factor relevante en la materialización y agravamiento de los riesgos de probidad administrativa.

Por tanto, la inexistencia de controles adecuados, la falta de supervisión efectiva o la inacción frente a alertas conocidas, deberán ser consideradas debilidades críticas del sistema de control interno, y tratadas como factores que incrementan la probabilidad y severidad del riesgo.

11. Documentación y Seguimiento de los Controles

Los controles asociados a riesgos de probidad administrativa deberán:

- Documentarse de manera clara y verificable
- Integrarse a los procedimientos institucionales
- Contar con responsables definidos
- Ser objeto de seguimiento periódico
  El seguimiento deberá enfocarse especialmente en los riesgos ubicados en las zonas naranjas y rojas del mapa de calor, priorizando aquellos de mayor criticidad institucional.

12. Riesgo Residual de Probidad Administrativa

El riesgo residual corresponde al nivel de exposición institucional que permanece una vez aplicados los controles existentes, considerando su efectividad real y la criticidad institucional del riesgo.
En materia de probidad administrativa, el riesgo residual no se limita a una reestimación mecánica de probabilidad e impacto, sino que refleja la exposición efectiva al daño institucional, reputacional y normativo.

12.1. Determinación del Riesgo Residual

La determinación del riesgo residual deberá considerar:

a. Severidad Inherente Ajustada

Incluye:

- Probabilidad inicial.
- Impacto estimado.
- Ajuste cualitativo aplicado.
- Persistencia histórica.
- Correlación con otros riesgos.

b. Efectividad Real de los Controles

La reducción del riesgo solo podrá justificarse cuando:

- El control esté correctamente diseñado.
- Exista evidencia verificable de su aplicación.

- Tenga cobertura adecuada.
- Actúe sobre la causa del riesgo.

Distinción clave:

- Controles detectivos → No reducen probabilidad inherente.
- Medidas reactivas → No reducen probabilidad futura.
- Correctivos estructurales → Sí pueden reducir probabilidad.

La sola existencia formal de un procedimiento no constituye reducción efectiva del riesgo.

c. Exposición Residual al Valor Público

Aun cuando existan controles, deberá evaluarse si la eventual materialización del riesgo:

- Compromete confianza ciudadana.
- Afecta legitimidad institucional.
- Debilita el deber de control.
- Puede generar repercusión pública significativa.

En tales casos, el impacto residual puede mantenerse elevado.

13. Ajuste Cualitativo del Riesgo Residual

En riesgos de probidad administrativa, la aplicación automática de reducción aritmética puede subestimar el riesgo real.

Por ello, previo a su clasificación definitiva, deberá aplicarse un ajuste cualitativo basado en:

- Impacto en el valor público.
- Velocidad de materialización.
- Persistencia o reiteración.
- Interdependencia con otros riesgos.
- Debilidad en el ejercicio del deber de control.

13.1. Principios Rectores del Ajuste

- **Principio de Criticidad Institucional**

No podrá reducirse automáticamente un riesgo que afecte dimensiones esenciales de legitimidad.

- **Principio de Prudencia**

Ante incertidumbre sobre efectividad real del control, se privilegiará estimación conservadora.

- **Principio de Coherencia Sistémica**

Debe evitarse análisis aislado cuando el riesgo tiene correlación estructural.

13.2. Resultado del Ajuste

El ajuste podrá implicar:

- Confirmar clasificación residual.
- Mantener nivel elevado.
- Elevar severidad residual.

No podrá reducirse a nivel bajo un riesgo cuyo impacto inherente haya sido clasificado como Mayor o Catastrófico si persisten vulnerabilidades.

14. Evaluación y Aceptación del Riesgo Residual

La aceptación del riesgo residual constituye decisión de gobernanza institucional, no meramente técnica.

Se aplicarán las siguientes reglas:

- Riesgo residual EXTREMO → No aceptable.
- Riesgo residual ALTO → Requiere plan obligatorio de tratamiento.
- Riesgo residual MODERADO → Aceptación condicionada y documentada.
- Riesgo residual BAJO → Aceptable con monitoreo.

La decisión deberá:

- Ser expresa.
- Estar fundada.
- Identificar responsable.
- Incluir medidas adicionales cuando corresponda.

15. Registro, Seguimiento y Escalamiento

El riesgo residual deberá:

- Registrarse en la matriz institucional.
- Vincularse a controles existentes.
- Contar con responsable designado.
- Establecer periodicidad de revisión.

Cuando se mantenga en nivel ALTO o EXTREMO:

- Deberá evaluarse escalamiento a la máxima autoridad.
- Se requerirá monitoreo reforzado.

La persistencia de riesgos residuales elevados puede evidenciar debilidad estructural del sistema de control interno.

En estos casos, deberán adoptarse medidas orientadas al fortalecimiento del sistema de control interno, reforzando una gestión preventiva, activa y responsable de los riesgos de probidad administrativa.

16. Apetito y Tolerancia al Riesgo de Probidad Administrativa

16.1. Marco Conceptual

En el ámbito de la probidad administrativa, el apetito de riesgo representa el nivel máximo de exposición que la institución está dispuesta a asumir en el cumplimiento de su mandato, sin comprometer:

- La legalidad del actuar administrativo.
- La confianza pública.
- La legitimidad institucional.
- El deber de probidad.
- El deber de control jerárquico.

Dado que los riesgos de probidad afectan directamente el valor público, el apetito institucional en esta materia es estructuralmente bajo.

La tolerancia al riesgo corresponde al margen específico de variación permitido respecto del nivel de riesgo residual ajustado, antes de exigir medidas adicionales.
El apetito y la tolerancia constituyen decisiones estratégicas de gobernanza, alineadas con principios de control interno y gestión del riesgo (COSO ERM; ISO 31000; INTOSAI).

16.2. Principios Aplicables a Riesgos de Probidad

a. Principio de Restricción

En materia de probidad administrativa, el apetito institucional es limitado, dado que estos riesgos comprometen directamente la integridad institucional.

b. Principio de No Tolerancia frente a Impacto Crítico

No existirá tolerancia cuando el riesgo residual:

- Comprometa gravemente la confianza pública.
- Afecte la legitimidad institucional.
- Evidencie debilidad en el deber de control.
- Presente reiteración histórica no corregida.

c. Principio de Proporcionalidad

La tolerancia podrá diferenciar entre:

- Riesgos de menor criticidad operativa.
- Riesgos que comprometen dimensiones sustantivas del mandato institucional.

16.3. Determinación del Nivel de Exposición al Riesgo Ajustado (NERA)

El apetito institucional se determinará en función del Nivel de Exposición al Riesgo Ajustado (NERA), entendido como el resultado final del riesgo residual luego de:

- Aplicar reducción por efectividad real de controles.
- Aplicar ajuste cualitativo.
- Considerar impacto en valor público

- **Clasificación del Nivel de Exposición Ajustado**

Cuadro Nº 22: Clasificación del Nivel de Exposición Ajustado

Nivel de Exposición al Riesgo Ajustado	Decisión de Apetito
NO ACEPTABLE (Na)	Fuera de apetito. Requiere intervención inmediata
MAYOR (Ma)	Fuera de apetito. Requiere plan obligatorio de tratamiento
MEDIA (Md)	Dentro de tolerancia condicionada, con monitoreo reforzado.
MENOR (Me)	Dentro de apetito institucional, con monitoreo periódico.

Regla reforzada:

Riesgos residuales clasificados como **EXTREMOS** o **ALTOS**, especialmente cuando afecten confianza pública o deber de control, se presumen fuera de apetito institucional.

16.4. Determinación de la Tolerancia

a. Tolerancia Cuantitativa

Podrá establecerse un margen técnico (por ejemplo, ±10% del NERA), siempre que:

- No implique reclasificación automática a nivel inferior.
- No afecte riesgos con impacto en valor público máximo.
- No se trate de riesgos con reiteración histórica.

b. Tolerancia Cualitativa

No existirá tolerancia cuando:

- El riesgo afecte directamente legitimidad institucional.

- Exista debilidad estructural no corregida.
- Se evidencie omisión del deber de control.
- El multiplicador cualitativo supere el umbral crítico (ej. > 2.0).

16.5. Relación entre Apetito, Tolerancia y Mapa de Calor

La integración operativa se realiza conforme a la siguiente lógica:

Cuadro Nº 23: Integración Mapa de Calor y Toma de Decisiones

Zona del Mapa Residual	Decisión de Apetito
Rojo	Fuera de apetito – intervención inmediata
Naranjo	Fuera de apetito – Plan obligatorio
Amarillo	Dentro de tolerancia condicionada
Fuera de mapa	Dentro de apetito

16.6. Gobernanza del Apetito y Tolerancia

La definición formal del apetito y tolerancia deberá:

- Ser aprobada por la máxima autoridad del servicio.
- Quedar documentada.
- Revisarse anualmente o ante cambios significativos.
- Alinearse con la política institucional de integridad.

La aceptación de riesgos residuales dentro del rango de tolerancia constituye una decisión estratégica, no meramente técnica.

16.7. Relación con el Ajuste Cualitativo

Cuando el multiplicador cualitativo arroje un valor superior a 2,0, el riesgo residual ajustado deberá presumirse fuera de apetito institucional, salvo justificación fundada.
Este criterio fortalece la coherencia entre:

- Evaluación técnica.
- Ajuste prudencial.
- Decisión de gobernanza.

17. Consideraciones Finales

La gestión de riesgos de probidad administrativa constituye un mecanismo preventivo esencial para la protección del valor público, la legitimidad institucional y el fortalecimiento del sistema de control interno.

Su implementación no es facultativa, sino una exigencia derivada del principio constitucional de probidad, del deber de control jerárquico y de los estándares modernos de gobernanza pública.

Un sistema basado exclusivamente en sanción individual es insuficiente.

La probidad se protege fortaleciendo el sistema, no solo reaccionando frente al evento.

VII. MANTENCIÓN Y MEJORAMIENTO DEL PROCESO DE GESTIÓN DE RIESGOS

El proceso de gestión de riesgos no debe concebirse como un instrumento estático, sino como un proceso vivo que requiere revisión, aprendizaje y mejoramiento continuo para seguir siendo eficaz, eficiente y pertinente frente a los cambios en el entorno interno y externo de las organizaciones públicas.

Este acápite busca consolidar un enfoque cíclico de gestión, asegurando la sostenibilidad del sistema en el tiempo, la coherencia con los objetivos institucionales, y el aprendizaje organizacional.

1. Actividades a Desarrollar Periódicamente

La organización debe establecer un plan sistemático de revisión del proceso de gestión de riesgos, que considere los siguientes puntos:

1.1. Fase Alcance, Contextos, Criterios

a. Establecer la Política de Gestión de Riesgos

Corresponde a la declaración de las intenciones y orientaciones globales de una organización en relación con la gestión del riesgo[13]. La política de riesgos se debe definir y documentar, aprobándose por la dirección y debe contener al menos los siguientes elementos:

- La razón fundamental de la organización gubernamental en materia de gestión del riesgo (el objetivo o propósito de la gestión de riesgos).
- Los enlaces entre los objetivos y las políticas de la organización y la política de la gestión del riesgo.
- La definición del Apetito al Riesgo.
- Las obligaciones de rendir cuentas y las responsabilidades en materia de gestión del riesgo.
- La manera en la que se tratan los intereses que entran en conflicto.
- El compromiso con el fin de tener disponibles los recursos necesarios para ayudar a aquellos con la obligación de rendir cuentas y responsables por la gestión del riesgo.
- La manera en la que se mide e informa el desempeño de la gestión del riesgo.
- El compromiso para revisar y mejorar la política de gestión del riesgo y el marco de trabajo, periódicamente y como respuesta a un evento o a un cambio de las circunstancias.

La Dirección debe asegurar que la política de riesgos se incluya y sea coherente con la política de calidad de la entidad, y que sea publicada y comunicada a través de todos los niveles

[13] NCH-ISO GUIA 73:2012

organizacionales, estableciendo responsables y plazo de las comunicaciones. En **Anexo Nº 3** se entrega un ejemplo de política de gestión de riesgos.

En esta fase se debe definir la política de gestión de riesgos y ser aprobada por el Jefe de Servicio mediante resolución exenta o documento equivalente. En el caso de estar dictada, se debe revisar, para determinar su consistencia con las políticas y objetivos estratégicos de la organización gubernamental, poniendo especial énfasis en que la política de riesgos considere todos los procesos que ejecuta y que sea consistente con la política de calidad de la entidad, si procede.

b. Establecer los Responsables y sus Roles

Se deben definir, documentar y aprobar los roles de las personas relacionadas con las siguientes materias:

- Iniciar acciones para prevenir o reducir los efectos de los riesgos.
- Controlar el tratamiento de los riesgos.
- Identificar y registrar cualquier problema relacionado con la gestión de los riesgos.
- Iniciar, recomendar o proveer soluciones a través de estrategias.
- Verificar a través del monitoreo la implementación de las soluciones contenidas en las estrategias.

En **Anexo Nº 7**, se presenta un ejemplo de asignación de roles y responsabilidades.

Es importante señalar que el Auditor Interno de la organización gubernamental no puede ser nombrado como responsable en estos temas, ya que se estaría afectando su objetividad e independencia al momento de auditar el funcionamiento y efectividad del Proceso de Gestión de Riesgos (actividad de aseguramiento). En **Anexo Nº 8** se entrega un resumen del rol de la auditoría interna en un Proceso de Gestión de Riesgos en el sector gubernamental, destacándose aquellas funciones que puede realizar y aquellas que no le están permitidas[14].

La organización gubernamental deberá definir los roles y las responsabilidades relacionados con el Proceso de Gestión de Riesgos, por el Jefe de Servicio mediante resolución exenta o documento equivalente. Para ello, se debe tener en cuenta el tamaño de la organización, su estructura y cultura organizacional, la jerarquía y la disponibilidad del personal para asumir posiciones de coordinación y/o responsabilidad. En caso de existir una asignación de roles y responsabilidades, esta debe analizarse para determinar si responde en forma adecuada a los requerimientos del proceso, examinando la necesidad de modificar roles, crear o eliminar instancias, mejorar la definición de responsabilidades, entre otros elementos. Siempre es importante considerar en este análisis el cambio de lineamientos y directrices que experimente la organización gubernamental cuando hay un cambio de Administración, ya sea a nivel de la Jefatura de la misma organización o a nivel de Gobierno. Por ende, se recomienda su adopción para el establecimiento del Proceso de Gestión de Riesgos.

[14] Se hace de acuerdo con la mirada del Instituto de Auditores Internos Global (IIA).

c. Establecer un Diccionario de Riesgos

A nivel teórico y práctico se considera la necesidad de formular un diccionario de riesgos para la entidad. En este caso, como se trata de organizaciones gubernamentales, el diccionario de riesgos confeccionado por el CAIGG puede resultar de utilidad para todas las organizaciones del Sector Público.

En general, siempre que sea necesario, la organización gubernamental puede incorporar conceptos adicionales propios, a fin de hacer más completo e ir actualizando el Diccionario de Riesgos, sin perjuicio de las medidas complementarias que al respecto pudiera tomar el CAIGG.

d. Alcance y Contexto de Gestión de Riesgo

Para la desagregación de procesos críticos y el modelamiento de riesgos, la organización gubernamental debe:

- Identificar los procesos que ejecuta la organización.

- Priorizar los procesos críticos según su nivel de contribución al cumplimiento de los Objetivos Estratégicos.

- Clasificar los procesos entre los procesos transversales definidos en este Documento Técnico.

- Identificar los subprocesos que componen los citados procesos críticos.

- Ponderar los subprocesos en relación con su importancia para el proceso crítico que componen.

  Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, las organizaciones gubernamentales deben ponderar y/o revisar las ponderaciones anteriores, considerando los siguientes puntos:

  - Todos los subprocesos identificados deben ponderarse.
  - La ponderación de todos los subprocesos debe sumar cien por ciento (100%).
  - La ponderación es reflejo de la importancia del proceso en el quehacer de la organización gubernamental, de ello que los subprocesos que contribuyen a generar productos estratégicos de dicha organización deberían tener mayor ponderación.
  - La justificación debe fundamentarse en algún criterio de los antes mencionados. No basta señalar en qué consiste el subproceso, ni tampoco es suficiente indicar que se trata de un subproceso clave al interior de la organización gubernamental, sino que es necesario señalar el porqué de su relevancia.
  - La ponderación y su justificación deben considerar la relevancia financiera y los recursos que involucran los procesos identificados.

- Dado lo anterior, la organización gubernamental debe definir las ponderaciones o revisarlas y mejorarlas, de acuerdo con lo señalado en el Capítulo V, número 1, numeral 1.1, letra e de este documento, teniendo presente que los cambios de políticas de Gobierno, las

modificaciones presupuestarias y la orientación en los lineamientos de la Dirección, las afectan directamente. En especial, debe considerarse el enfoque de los directivos y la relación de los procesos con el cumplimiento de la misión institucional de la organización gubernamental y los recursos financieros involucrados.

- Identificar las etapas que componen los subprocesos del proceso crítico (si corresponde).
- Identificar los objetivos o finalidades que tienen cada una de las etapas o subprocesos, según corresponda. Esta información debe derivarse de documentación formal de la organización gubernamental, como reglamentos e instructivos o de información emanada de los encargados de los procesos críticos.

1.2. Fase Evaluación del Riesgo

- Identificar oportunidades

  Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, se debe identificar oportunidades a nivel global de procesos de negocio. Es importante la realización de esta actividad, puesto que las oportunidades sirven a la institución para retroalimentar las estrategias, en especial para incorporar los nuevos énfasis de Gobierno.

- Identificar los riesgos que pueden impedir, afectar o retrasar el logro de los objetivos de la etapa o subproceso según corresponda. Para esta identificación se pueden utilizar diversas herramientas como los talleres o la lluvia de ideas (**Anexo N° 10**).

  Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, la organización gubernamental debe identificar los riesgos o revisar y mejorar su identificación de riesgos, poniendo especial énfasis en los siguientes puntos:

  - Identificar o actualizar los riesgos, considerando los cambios normativos, presupuestarios o de los lineamientos del Gobierno o de la dirección, en especial los nuevos enfoques y énfasis de Gobierno y de las autoridades de la organización gubernamental u otras autoridades externas a aquella.
  - Identificar en la forma más completa y desagregada posible los riesgos que se relacionan a una etapa dentro de un proceso. Para ello se sugiere examinar las actividades al interior de las etapas, identificando los riesgos que se asocian a dichas actividades.
  - Identificar en forma prioritaria los riesgos asociados con aspectos económicos y financieros, considerando los recursos involucrados en los procesos y subprocesos.
  - Considerar que una etapa puede tener, y en general es así, más de un riesgo.
  - Considerar que una buena y completa descripción del objetivo operativo de la etapa facilita la identificación de riesgos.

- Clasificar los riesgos por tipo y origen definidos en este Documento Técnico.

  Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, se debe señalar, de acuerdo con la tipología entregada, a qué tipo genérico de riesgo corresponde el riesgo operativo determinado y cuál es su fuente (externa o interna), como se señala en el ejemplo del **Cuadro Nº 8**. Lo anterior implica poner un especial cuidado en dilucidar si el riesgo identificado, tiene su origen al interior de la entidad, por lo tanto, es

manejable por esta, o bien, si en caso contrario se origina externamente y solo pueden tomarse acciones paliativas que afecten indirectamente el nivel de riesgo. Por ejemplo, cuando se trata de decisiones que son de responsabilidad de otras reparticiones del Estado.

La clasificación y/o la revisión de las tipologías de riesgo deben tener en consideración los siguientes puntos:

- Todos los riesgos deben tener asignado sólo una fuente, interna o externa, de acuerdo con el origen que sea más relevante para el riesgo.
- Todos los riesgos deben clasificarse sólo en una tipología.
- Las tipologías deben asignarse de acuerdo con dónde se originan los riesgos, no se deben asignar según sus consecuencias. Por ejemplo, si se incumple la normativa de Gobierno Electrónico y ello afecta a los usuarios en la accesibilidad y disponibilidad, este hecho afectará la imagen de la entidad, pero se trata de un riesgo de tipo tecnológico.

Cuando existan dudas o diferencias que surjan en la tipificación de los riesgos específicos, estas deberán consultarse y discutirse con el respectivo asesor del CAIGG.

- Identificar señales de alerta de delitos LA/FT/DF asociados a los riesgos.

  Evaluar y determinar si es necesario actualizar las señales de alerta de delitos LA/FT/DF que afectan a la organización, estén o no incluidas en la Matriz de Riesgos Estratégica.

- Valuar los riesgos en relación con su probabilidad e impacto y a su nivel de severidad.

  El **Anexo N° 9** contiene una definición global y transversal para determinar los niveles de riesgos que se pueden tomar en las entidades públicas determinada por el CAIGG. Sin perjuicio de lo anterior, cada entidad debería evaluar en forma periódica cuán aplicable es la referida definición a su entidad, de acuerdo con sus actuales escenarios y la naturaleza y características organizacionales al momento de la evaluación.

- Identificar los controles claves asociados a los riesgos identificados, respondiendo las preguntas ¿qué control se realiza?, ¿cómo se realiza?, ¿quién los realiza?, ¿cuándo o en qué oportunidad se ejecuta el control?

  Describir y analizar los controles claves que mitigan los riesgos después de un análisis profundo de los mismos, detallando **qué se hace, cómo se hace, quién lo hace y cuándo lo hace**. (**Anexo N° 16**) Por ejemplo: Se realiza una visación de los contratos de mutuo (qué se hace) a través de comparar una muestra de al menos 30% de los contratos firmados con las resoluciones y la información del sistema (cómo se hace); dicha labor se realiza por el Jefe de la División de Créditos (quién lo hace) en forma semestral (cuándo lo hace) emitiendo un reporte al Jefe de Servicio (cómo se hace).

  En la identificación y revisión de los controles que se asocian a los riesgos, se sugiere:

  - Identificar controles claves (ver definición en el **Anexo Nº 16**). Para ello, es necesario establecer la definición del control clave con un breve detalle de las actividades del control realizado.

- Mejorar la descripción de los controles, señalando la norma o guía que lo instruye, quién lo realiza, qué actividades desarrolla, cómo las ejecuta y cuándo y cómo se evidencia su cumplimiento (registros documentales o electrónicos en el sistema).
- Analizar si está documentado, esto es, formalizado por escrito.
- Analizar si existe segregación de funciones, esto es, si la persona que autoriza es distinta a la que ejecuta o registra la operación.
- En base a la descripción del control realizado, clasificar en forma consistente la efectividad del diseño, es decir, su periodicidad, oportunidad y automatización.
- Considerar que los controles claves que se identifican deben estar directamente relacionados con el riesgo que teóricamente mitigan.
- Valuar los controles claves en relación con la efectividad de su diseño.

- Determinar la exposición al riesgo por riesgo, etapa, subproceso y proceso, según corresponda.

  En el caso de haber trabajado en la implementación de procesos de gestión de riesgos con anterioridad en la organización gubernamental, es necesario revisar nuevamente la desagregación de procesos, y subprocesos, así como los objetivos, riesgos y controles, determinando si esta desagregación y la identificación de riesgos y controles son adecuadas y corresponde a la realidad de la entidad. Otro punto en los que debe tenerse especial consideración, son en los cambios que hayan enfrentado los lineamientos de la organización gubernamental, considerando que las nuevas autoridades o funciones, en los casos que así sean, aportarán nuevos enfoques y énfasis que hay que tener en cuenta en la Gestión de Riesgos.

1.3. Fase Tratamiento del Riesgo

- Ranking de procesos, de subprocesos y etapas

  Para el adecuado desarrollo del Proceso de Gestión de Riesgos, la organización gubernamental debe hacer un ranking de procesos, de subprocesos y etapas. Se sugiere la utilización de los **Cuadros Nºs 10 y 11,** respectivamente, como apoyo para el señalado ranking.

  Es importante que, en base la información proporcionada por los Ranking de Procesos y Subprocesos (incluyendo el Ranking de Etapas), la organización gubernamental determine qué etapas, subprocesos y procesos serán abordados con acciones para tratar los riesgos específicos. Dicha determinación debe fundamentarse debidamente, en consideración de aquellos riesgos para los cuales no se tomarán acciones para disminuir los niveles de riesgo. Para una adecuada fundamentación, se deberán considerar variables tales como la importancia estratégica de los procesos y subprocesos, aspectos presupuestarios, énfasis de las autoridades y todas aquellas variables que permitan justificar adecuadamente su tratamiento versus las materias que no serán abordadas con planes de tratamiento.

- Aspectos Relevantes para el Tratamiento de Riesgos

  Para un adecuado desarrollo del Proceso de Gestión de Riesgos, la organización gubernamental debe confeccionar un Plan de Tratamiento de Riesgos, que contenga todos los riesgos críticos de dicha entidad, de acuerdo con la priorización realizada.

El Plan de Tratamiento deberá realizarse teniendo en consideración los siguientes puntos:

- Los riesgos escogidos para el tratamiento deben ser adecuados para gestionar el riesgo del o los procesos y subprocesos priorizados, esto implica que dentro de un proceso deberían tratarse los riesgos relevantes o críticos que faciliten que éste mejore de manera de mantener su nivel de riesgos (a nivel de proceso) dentro de los límites tolerables.
- Las estrategias escogidas deberían ser: reducir, aceptar o compartir, teniendo presente que las estrategias de aceptar o evitar, no tienen efecto sobre la severidad del riesgo o la efectividad del control, y que la estrategia evitar es de aplicación muy limitada en el sector público.
- Las acciones definidas deben ser aptas para mitigar el riesgo al cual se asocian, de manera que esas acciones actúen de manera directa en el riesgo que se espera afectar.
- Cuando se requiera mejorar un control como medida de tratamiento de los riesgos, la acción debe demostrar que el control actual se actualizará o complementará, en ningún caso que se mantendrá.
- Los indicadores deben ser de resultado y señalar explícitamente qué es lo que se quiere medir. Debe expresarse como una medida y establecer las variables y operaciones que se deben realizar para el cálculo del indicador.
- La meta debe ser el valor deseado del indicador que se espera alcanzar.
- El verificador debe ser apto para dar seguridad de que se alcanzó la meta.

Para mayor claridad de los puntos anteriores, ver un ejemplo en **Anexo Nº 18**.

De acuerdo con lo anterior, debe emitirse un Plan de Tratamiento que contendrá las medidas a adoptarse ante los riesgos críticos de la organización gubernamental. Se sugiere el uso del formato del **Cuadro Nº 24**:

Cuadro Nº 24: Formato para informar del plan de tratamiento de los riesgos priorizados

Proceso Transversal (1)	Proceso (2)	Ranking de Procesos (3)	Subproceso (4)	Etapa (5)	Riesgo Específico (6)	Fuente del Riesgo (7)	Tipo de Riesgo (8)	Estrategia Genérica (9)	Descripción de la Estrategia a Aplicar (10)	Efecto Potencial en la Severidad de Riesgo y/o Efectividad del Control (11)	Responsable de la Estrategia (12)	Plazo (13)	Indicador de Logro (14)	Periodo Medición del Indicador (15)	Meta (16)	Evidencia que se Observará (17)

Descripción de la información solicitada en el formato dispuesto en el cuadro Nº 24	
N° Descriptor	**Significado**
(1)	Proceso genérico, transversal o megaproceso al cual corresponde el proceso priorizado, de acuerdo a la clasificación del documento (Cuadro Nº 1).
(2)	Denominación específica que el proceso tiene en la Organización Gubernamental.
(3)	Prioridad de tratamiento del proceso, de acuerdo al nivel de exposición al riesgo.
(4)	Subprocesos que conforman el proceso priorizado.
(5)	Etapas que conforman cada uno de los subprocesos del proceso priorizado.
(6)	Riesgos que se identifican en la etapa, en relación a actividades que en dicha etapa se llevan a cabo.

Descripción de la información solicitada en el formato dispuesto en el cuadro Nº 24	
(7)	Origen externo o interno de los riesgos, de acuerdo al control que tiene la Organización Gubernamental de la fuente que los produce.
(8)	Clasificación del riesgo, de acuerdo a la tipología que entrega el documento en el Cuadro Nº 4.
(9)	Tipo de estrategia que se adoptó para tratar ese riesgo de acuerdo al punto 5.2 (evitar, reducir, compartir, aceptar).
(10)	Detalle de la estrategia genérica que se va a utilizar. Pormenorizar las acciones y actividades que se desarrollarán para llevar a cabo la estrategia genérica.
(11)	Señalar si la estrategia apunta a disminuir la severidad del riesgo (probabilidad, impacto o ambos) y/o a potenciar el control y de qué manera.
(12)	Señalar quien es la persona y cargo responsable de la implementación de las acciones específicas de la estrategia.
(13)	Definir en qué plazo se debe implementar la estrategia.
(14)	Corresponde a la forma cuantitativa o cualitativa como se evalúa el nivel de cumplimiento de la estrategia definida. Debe tratarse de un indicador de resultado, que demuestre cómo la estrategia mitiga el riesgo al cual se asocia.
(15)	Señalar periodos en que se va a medir el indicador dependiendo de la naturaleza del mismo (mensual, trimestral, semestral, etc.)
(16)	Resultado tangible que se espera lograr con la implementación de la estrategia.
(17)	Documento o instrumento que se utilizará en la medición del indicador.

1.4. Fase Seguimiento y Revisión

Sin perjuicio a que la Fase de Monitoreo y Revisión es transversal al resto de las fases del Proceso de Gestión de Riesgos, se requiere que la organización gubernamental realice el monitoreo en base al Plan de Tratamiento que definió. Se sugiere que se utilice el formato que se señala en el siguiente **Cuadro N° 25**.

Cuadro Nº 25: Formato Básico para Informar del Monitoreo de las Estrategias de Tratamiento de los Riesgos

Proceso transversal	Proceso	Subproceso	Etapa	Riesgo específico	Estrategia genérica	Descripción de la estrategia a aplicar	Periodo de evaluación de implementación de la estrategia (a)	Resultados de la medición de la metas (b)	Evidencia del cumplimiento (c)	Proyecciones de cumplimiento (d)	Recomendaciones (e)

Descripción de la información solicitada en el formato dispuesto en el Cuadro Nº 14 (sólo aquellos conceptos no explicados con ocasión del formato Nº 15)	
Número de descriptor	**Significado**
(a)	Señalar en qué fecha se evaluó la implementación de la estrategia.
(b)	Señalar el resultado que se obtuvo de la medición de las metas. (Cumplida, parcialmente cumplida, porcentaje de cumplimiento, etc.)
(c)	Expresar y detallar en que documentos o que información se utilizó para tener evidencia suficiente y adecuada del cumplimiento.
(d)	En caso de no haberse cumplido totalmente la meta, como se proyecta que será el cumplimiento. (En unidades de tiempo, o si no se podrá cumplir).
(e)	Sugerencias que realiza el responsable del monitoreo y revisión para que se obtenga el logro de la meta, o se mejore en términos de oportunidad y calidad.

1.5. Fase Comunicación y Consulta

Algunos ejemplos de criterios e indicadores (la organización gubernamental debe diseñar sus propios indicadores de acuerdo con su naturaleza y necesidades) que pueden establecerse en relación con el análisis de la información derivada del Proceso de Gestión de Riesgos, se muestran a continuación en el **Cuadro Nº 26**.

Sin perjuicio de la periodicidad en que el Jefe de Servicio y el CAIGG requieran el envío de los resultados de los indicadores y en general de los distintos reportes, la organización debería definir responsables y plazos para monitorear los cambios de estos resultados y así obtener información oportuna que ayude a la toma de decisiones de la Dirección.

Cuadro Nº 26: Ejemplos de Criterios e Indicadores para Análisis de Información del Proceso de Gestión de Riesgos

Criterio	Posibles Indicadores para Análisis (La lista no es taxativa)	Responsable	Plazos
Asociados a Comprensión del Proceso de Gestión de Riesgos			
Calidad Cursos y Talleres	• Áreas con mayor cantidad de participantes. • Materias de mayor complejidad para los alumnos. • Áreas de mejor rendimiento en el curso.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Nivel de Aplicación	• Áreas que mejor desarrollan el Proceso. • % de personas involucradas por área.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Asociados a los Reportes del Proceso de Gestión de Riesgos			
Oportunidad Reportes	• Cumplimiento con la distribución del reporte. • Días de retraso respecto del Plan de comunicación.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Calidad Contenido	• Exactitud de la información del reporte. • Completitud de análisis del reporte. • Nivel de medidas correctivas y preventivas comprometidas en reporte de tratamiento.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Asociados a la Matriz de Riesgos Estratégica del Proceso de Gestión de Riesgos			

Criterio	Posibles Indicadores para Análisis (La lista no es taxativa)	Responsable	Plazos
Severidad del Riesgo	• Procesos con más altas severidades del riesgo. • Subprocesos con más altas severidades de riesgo. • Etapas con más altas severidades de riesgo.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Exposición al Riesgo	• Procesos con más altas exposiciones al riesgo. • Subprocesos con más altas exposiciones al riesgo. • Etapas con más altas exposiciones al riesgo.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En los meses de enero y octubre de cada año.
Impacto al Riesgo	• Procesos con riesgos de impactos más altos. • Subprocesos con riesgos de impactos más altos. • Etapas con riesgos de impactos más altos.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Tipos de Riesgos	• Tipologías de Riesgos que más se repiten. • Tipos de riesgos con mayor exposición. • Tipos de riesgos con mayor impacto.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Controles	• Procesos con controles más efectivos. • Procesos con controles menos efectivos. • Riesgos extremos con controles menos efectivos.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Ranking	• Procesos en los primeros lugares del ranking y su relación al negocio. • Procesos en los primeros lugares del ranking y su relación al soporte. • Procesos priorizados y profundidad del levantamiento realizado.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Asociados a Otras Dimensiones del Proceso de Gestión de Riesgos			
....	....	....	....

Para un adecuado desarrollo del Proceso de Gestión de Riesgos, se debe permanentemente revisar y mejorar la información que fluye en el Proceso de Gestión de Riesgos orientándose a que esta refleje un uso adecuado en dicho proceso. Para lo anterior, el Jefe de Servicio debe aprobar un Plan de Comunicación y Consulta que deberá implementarse al inicio del Proceso de Gestión de Riesgos[15], considerando los plazos y roles definidos por la organización y que contenga al menos los siguientes componentes:

- Definir Componente Reportes Sobre Temas Relativos al Riesgo

  - Tipo, contenido y periodicidad de reportes de análisis de indicadores relacionados con el Proceso de Gestión de Riesgos en general. Se recomienda examinar los ejemplos de criterios e indicadores de la información del Proceso de Gestión de Riesgos que se muestran en el **Cuadro Nº 14.**

  - Tipo, contenido y periodicidad de reportes de análisis relacionados con la Matriz de Riesgos Estratégica al Jefe de Servicio y responsables de las áreas en la organización. Se recomienda formular un resumen de los principales puntos o temas de interés que

[15] Sin perjuicio de las actualizaciones posteriores que se requiera hacer al Plan de Comunicación y Consulta.

arroja el examen y análisis de la Matriz de Riesgos Estratégica, como por ejemplo; áreas que no han informado de sus procesos y riesgos oportunamente, procesos más críticos de la institución, de mayor severidad, menos controlados, los que aparecen excesivamente controlados en relación con su severidad, etc. Este reporte puede contener información de los indicadores generales del Proceso de Gestión de Riesgos, como también de otras fuentes. El reporte debería ser elaborado por personal que se relacione con el Proceso de Gestión de Riesgos y debería ser remitido al Jefe de Servicio al menos una vez en el año y al CAIGG cuando éste lo solicite.

- Tipo, contenido y periodicidad de reportes de actualización del análisis de riesgos. Incluir nuevos riesgos o riesgos emergentes, cambios significativos en la probabilidad o el impacto de los riesgos existentes, cambios en factores de riesgos, etc.

- Tipo, contenido y periodicidad del reporte del Plan de Tratamiento de Riesgos al Jefe de Servicio y responsables de las áreas en la organización. Tener presente los elementos considerados en el punto V.- Plan de Tratamientos, incluido en este documento técnico.

- Definir Componentes de las Comunicaciones y Consultas Internas y Externas

El Jefe del Servicio debe aprobar formalmente los siguientes temas:

- Identificar usuarios o clientes internos y externos, y su nivel e importancia para el Proceso de Gestión de Riesgos.
- Definir qué tipo de información se espera recibir y remitir en el proceso.
- Definir roles y responsables de la calidad y confiabilidad para la información a recibir y remitir.
- Definir periodicidad para la información a recibir y remitir.
- Identificar y definir sistemas, canales y mecanismos para manejar la información de gestión de riesgos al interior de la organización y para remitirla externamente.
- Definir qué tipo de reportes tendrá el proceso. Definir Tipo de análisis que se incluirán en los reportes.
- Definir el procedimiento de cómo se realizará la comunicación, identificar los soportes y tecnologías requeridas.
- Definir cómo y quiénes tendrán acceso a la comunicación, señalar los criterios para definir perfiles por tipo de información.
- Definir cómo se recolectarán opiniones que genere la comunicación, espacios de participación, forma como se hará efectiva la participación.

El Plan de Comunicación y Consulta deberá enviarse al menos anualmente al Jefe de Servicio y al CAIGG cuando éste lo solicite.

1.6. Fase Registro e Informe

Para una adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, la organización gubernamental deberá definir en un procedimiento los registros que llevará con la finalidad de documentar dicho proceso, indicando al menos:

- Tipo de registro.
- Contenido del registro.

- Responsable del registro.
- Cómo y quiénes tendrán acceso al registro.
- Cómo y dónde se almacenarán y respaldarán los registros.
- Por cuánto tiempo se deben almacenar y quién puede destruirlos y reemplazarlos.
- Si existen temas sensibles en él o los registros y qué medidas se tomarán en dicho caso.

1.7. Reportes del proceso de gestión de riesgos al Consejo de Auditoría Interna General de Gobierno

En el **Anexo N° 19** se presenta un ejemplo del formato tipo de la Matriz de Riesgos Estratégica y en el **Anexo N° 20** se muestra un ejemplo de levantamiento de información de un proceso.

El CAIGG podrá definir en forma periódica qué reportes derivados del Proceso de Gestión de Riesgos desarrollado por las organizaciones gubernamentales deben ser reportados, así como la oportunidad y formato de dichos reportes.

VIII. REFERENCIAS NORMATIVAS Y BIBLIOGRÁFICAS

1. Referencias Normativas

- Constitución Política de la República de Chile.
- Congreso Nacional de Chile. (1986). **Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado**.
- Congreso Nacional de Chile. (1989). **Ley N° 18.834, Estatuto Administrativo**.
- Congreso Nacional de Chile. (2003). **Ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos**.
- Congreso Nacional de Chile. (2016). **Ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de interés**.
- Congreso Nacional de Chile. (2023). **Ley N° 21.634, que moderniza el sistema de compras públicas**.
- Ministerio de Hacienda. (2015). **Oficio Circular N° 20. Orientaciones para el Sector Público en relación con el inciso sexto del artículo 3° de la Ley N° 19.913**.
- Ministerio de Hacienda. (2015). **Guía de recomendaciones para el sector público en la implementación de sistemas preventivos contra delitos funcionarios, lavado de activos y financiamiento del terrorismo**.
- Unidad de Análisis Financiero. (s.f.). **Guía de señales de alerta para la detección de operaciones sospechosas**. Disponible en: https://www.uaf.gob.cl

2. Referencias Técnicas y Metodológicas

- Consejo de Auditoría Interna General de Gobierno (CAIGG). (2009). **Documento Técnico N° 41: Gestión de Riesgos**.
- Consejo de Auditoría Interna General de Gobierno (CAIGG). (2010). **Documento Técnico N° 45: Gestión de Riesgos**.
- Consejo de Auditoría Interna General de Gobierno (CAIGG). (2014). **Documento Técnico N° 59: Gestión de Riesgos**.

- Consejo de Auditoría Interna General de Gobierno (CAIGG). (2022). **Documento Técnico N° 70 v 3: Gestión de Riesgos**.
- Consejo de Auditoría Interna General de Gobierno (CAIGG). (2025). **Guías de Gestión y Servicios de Auditoría Interna (GGSAI).**
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). **Internal Control – Integrated Framework**.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). **Enterprise Risk Management – Integrating with Strategy and Performance**.
- Institute of Internal Auditors (IIA). (2010). **Practice Guide: Assessing the Adequacy of Risk Management Using ISO 31000**.
- Institute of Internal Auditors (IIA). (2011). **International Professional Practices Framework (IPPF)**.
- Institute of Internal Auditors (IIA). (2024). **Global Internal Audit Standards**.
- International Organization for Standardization. (2013). **ISO/TR 31004: Risk Management – Guidance for the Implementation of ISO 31000**.
- International Organization for Standardization. (2018). **ISO 31000: Risk Management – Guidelines**.
- International Organization for Standardization. (2019). **ISO 31010: Risk Management – Risk Assessment Techniques**.
- Instituto Nacional de Normalización. (2012). **NCh-ISO Guía 73:2012. Gestión del Riesgo – Vocabulario**.
- Instituto Nacional de Normalización. (2014). **NCh-ISO 31004:2014. Gestión del Riesgo – Orientación para la implementación de ISO 31000**.
- International Organization of Supreme Audit Institutions (INTOSAI). (2019). **INTOSAI GOV 9100 – Guidelines for Internal Control Standards for the Public Sector.**
- Organisation for Economic Co-operation and Development (OECD). (2017). **OECD Recommendation on Public Integrity.**
- Institute of Risk Management. (2018). **Risk Governance Guidance for Boards and Senior Management.**
- Instituto Nacional de Normalización. (2018). **NCh-ISO 31000:2018. Gestión del Riesgo – Directrices**.
- Instituto Nacional de Normalización. (2020). **NCh-ISO 31010:2020. Gestión del Riesgo – Técnicas de evaluación del riesgo**.
- Instituto de Auditores Internos de España. (2013). **Definición e implantación del apetito de riesgo**.
- Open Compliance and Ethics Group (OCEG). **GRC Capability Model – Red Book 3.0**.
- Organisation for Economic Co-operation and Development (OECD). (2015). **G20/OECD Principles of Corporate Governance**.
- OECD. (2014). **Risk Management and Corporate Governance**.

ANEXO Nº 1

CONCEPTOS SOBRE DIMENSIONES O CRITERIOS CUALITATIVOS ADICIONALES EN LA EVALUACIÓN DE RIESGOS

El nivel de severidad o gravedad de un riesgo, utilizado para determinar su priorización según la literatura especializada, se entiende como una función de todos los criterios que la organización decida emplear en su evaluación. Si bien los criterios más comúnmente utilizados son el impacto y la probabilidad, las organizaciones pueden incorporar otros para enriquecer el análisis, dependiendo del nivel de madurez de su proceso de gestión de procesos. A continuación, se describen algunos que pueden ser aplicados al sector público en mayor o menor medida (la lista no es taxativa):

- Vulnerabilidad.
- Volatilidad.
- Velocidad (que comprende la rapidez de reacción y la rapidez de recuperación).
- Interdependencia.
- Correlación.
- Persistencia.
- Impacto en el Valor Público.

- **Vulnerabilidad**

La vulnerabilidad es una medida de cuán susceptible es una organización a un riesgo determinado. Esto depende del nivel de preparación, agilidad y adaptabilidad de la organización. Dada esta descripción, es claro que existe una relación estrecha entre vulnerabilidad e impacto, debido a que, a mayor vulnerabilidad, mayor será el impacto probable. Este análisis resulta útil para comprender el riesgo e identificar una respuesta adecuada.

- **Volatilidad**

En algunos casos, la probabilidad de que un riesgo se active varía según la volatilidad de la situación. Cuando las condiciones fluctúan, es más difícil predecir la probabilidad de un evento determinado. Es probable que un riesgo de este tipo tenga una mayor prioridad para la gestión del riesgo debido a su mayor imprevisibilidad.

- **Velocidad**

Algunos análisis incluyen el criterio de velocidad del riesgo (o rapidez de aparición). Esta es una medida del tiempo de advertencia previa y de preparación que puede tener una organización entre la ocurrencia del evento y su impacto. Puede dividirse en rapidez de reacción y rapidez de

recuperación. El tiempo entre la ocurrencia del evento y su impacto en la organización a veces se conoce como proximidad.

- **Interdependencia**

Es importante no considerar los riesgos de manera aislada, sino también en combinación. La materialización de dos o más riesgos puede afectar a la organización de forma distinta a la suma de sus impactos individuales y puede depender de si los eventos ocurren de manera simultánea o consecutiva.

Por ejemplo, las centrales nucleares en Japón están preparadas para terremotos y tsunamis. Sin embargo, la concurrencia de ambos eventos puede permitir que una ola supere las defensas ya debilitadas por los temblores. Otro ejemplo: los controles financieros rutinarios suelen exigir la segregación de funciones clave para evitar que un empleado ordene bienes para uso personal. Sin embargo, si dos o más individuos deciden coludirse para cometer dicho fraude, es mucho más difícil de detectar. Las causas de los eventos de riesgo interdependientes no están relacionadas entre sí.

- **Correlación**

La correlación es similar a la interdependencia y se refiere a la conexión entre dos o más riesgos. En este caso, en lugar de una dependencia mutua de riesgos que desencadena nuevos riesgos potenciales, varía el impacto o la probabilidad de los riesgos. Por ejemplo, las debilidades en una economía nacional pueden generar riesgos cambiarios y aumentar los costos de bienes y servicios comercializados internacionalmente. Estos costos pueden aumentar la necesidad de endeudamiento. Los factores económicos subyacentes que provocan fluctuaciones en los tipos de cambio también pueden estar asociados con tasas de interés más altas y mayores dificultades para acceder al crédito. A diferencia de la interdependencia, las causas de los riesgos correlacionados sí están relacionadas.

Las interacciones entre eventos de riesgo (tanto interdependencias como correlaciones) pueden representarse en una cuadrícula, con cada riesgo encabezando todas las filas y columnas. Cuando dos riesgos se cruzan en la cuadrícula, existe el potencial de un riesgo aún mayor. Por ejemplo, una expansión o recesión económica probablemente desencadene, incremente o coincida con una amplia gama de otros eventos de riesgo relacionados con los costos de endeudamiento, los precios de materias primas y la demanda de bienes y servicios.

- **Persistencia**

Es la capacidad de un riesgo de mantenerse vigente, reaparecer o resistir los esfuerzos de mitigación en el tiempo. Refleja la tendencia del riesgo a prolongarse estructuralmente dentro de la organización, independientemente de los controles implementados, y sugiere la existencia de condiciones subyacentes (culturales, operativas o sistémicas) que favorecen su continuidad o reaparición.

Este criterio permite evaluar no solo la duración del riesgo, sino también la resiliencia negativa del mismo: su capacidad de adaptarse o mutar frente a intervenciones, haciendo que su

eliminación definitiva sea compleja. Un riesgo con alta persistencia puede parecer controlado temporalmente, pero volver a manifestarse debido a debilidades estructurales no resueltas.

- **Impacto en el Valor Público (variable específica para el sector público)**

En el contexto del sector público, además de las variables tradicionales de impacto y probabilidad y las cualitativas adicionales, es posible incorporar un criterio específico que se refiere al impacto del riesgo en el valor público. Este corresponde al grado en que un riesgo puede afectar la creación, protección o sostenimiento del valor público que generan las instituciones estatales a través de sus políticas, programas y servicios.

La incorporación del impacto en el valor público en la evaluación del riesgo permite priorizar aquellos eventos que no solo amenazan la gestión interna, sino también el valor que la entidad pública entrega a la sociedad, fortaleciendo la alineación con las NOGAI y los principios de gobernanza, integridad y sostenibilidad del Estado.

El impacto en el valor público puede manifestarse en diversas dimensiones:

- **Confianza ciudadana:** Pérdida o deterioro de la percepción de integridad, transparencia y legitimidad institucional.
- **Cumplimiento del mandato público:** Riesgos que impidan el logro de los objetivos estratégicos, metas de política pública o compromisos internacionales.
- **Eficiencia y eficacia del gasto público:** Riesgos que generen uso ineficiente, duplicación o desviación de recursos fiscales.
- **Equidad y bienestar social:** Riesgos que afecten la entrega oportuna, inclusiva y de calidad de servicios públicos esenciales.
- **Sostenibilidad institucional:** Riesgos que afecten la continuidad, capacidad técnica o resiliencia de la organización pública.

Tabla Nº 1: Escala Cualitativa de las Variables Adicionales para Evaluación de Riesgos

Variable	Categoría	Ponderación	Descripción Mejorada
Vulnerabilidad	Baja (1)	A definir	El proceso o población afectada cuenta con mecanismos robustos de defensa, respaldo institucional, protocolos activos y flexibilidad operativa.
	Media (2)		Existen controles o mecanismos, pero son parciales, desactualizados o con limitaciones de cobertura o aplicabilidad.

Variable	Categoría	Ponderación	Descripción Mejorada
	Alta (3)		Se evidencia exposición crítica por falta de preparación, dependencia tecnológica o institucional, o ausencia de planes de contingencia efectivos.
Volatilidad	Baja (1)	A definir	El riesgo presenta comportamiento estable y predecible; responde de forma constante ante condiciones similares.
	Media (2)		El riesgo puede variar ante ciertos factores internos o externos, pero sus fluctuaciones son generalmente controlables.
	Alta (3)		El riesgo se manifiesta de manera errática, con alta sensibilidad a variables externas e incapacidad para anticipar sus efectos.
Velocidad	Baja (1)	A definir	El impacto del riesgo es progresivo y permite una ventana de reacción mayor a dos semanas sin consecuencias graves inmediatas.
	Media (2)		El impacto se desarrolla en un plazo intermedio (3 días a 2 semanas), lo que exige respuesta diligente pero no urgente.
	Alta (3)		El riesgo genera efectos severos en menos de 72 horas, exigiendo reacción inmediata y protocolos activados de forma automática.
Interdependencia	Baja (1)	A definir	El riesgo puede gestionarse internamente sin depender de otros procesos, actores o sistemas externos.
	Media (2)		Existen vínculos con algunos procesos o sistemas externos, pero el riesgo puede aislarse en escenarios normales.
	Alta (3)		El riesgo se amplifica o se propaga por conexiones operativas, tecnológicas o institucionales con terceros o áreas críticas.
Persistencia	Baja (1)	A definir	El riesgo ha sido erradicado o controlado de forma sostenible, sin recurrencias tras la implementación de acciones correctivas.

Variable	Categoría	Ponderación	Descripción Mejorada
	Media (2)		El riesgo ha sido parcialmente mitigado, pero persisten factores estructurales que favorecen su reaparición bajo ciertas condiciones.
	Alta (3)		El riesgo es crónico, sistémico o cultural; ha reaparecido de forma recurrente a pesar de diversos esfuerzos de control.
Correlación	Baja (1)	A definir	El riesgo ocurre de forma aislada y no está relacionado con otros factores económicos, sociales o políticos relevantes.
	Media (2)		El riesgo está condicionado por algunos factores del entorno, pero su ocurrencia aún depende del contexto interno.
	Alta (3)		La manifestación del riesgo está estrechamente vinculada a variables externas (económicas, políticas, sociales, climáticas), lo que complica su predicción y gestión.
Impacto en Valor Público	Baja (1)	A definir	El riesgo, aunque se materialice, no genera afectación significativa al mandato, reputación ni confianza pública de la institución.
	Media (2)		Puede ocasionar deterioro parcial de la percepción institucional, incumplimientos menores de mandato o afectación limitada de servicios esenciales.
	Alta (3)		Genera una afectación severa al mandato, confianza ciudadana, credibilidad institucional, legitimidad del Estado o la equidad en la provisión de servicios públicos.

Método de evaluación ajustada de la Severidad del Riesgo (Riesgo Inherente) y Exposición al Riesgo (Riesgo Residual)

1. Evaluación tradicional de la Severidad del Riesgo

Se calcula como el producto entre la probabilidad y el impacto del evento de riesgo, utilizando una escala de 1 a 5.

Severidad del Riesgo Tradicional = Probabilidad × Impacto

- **Probabilidad:** mide la posibilidad de que el evento ocurra.
- **Impacto:** estima las consecuencias si el evento se materializa.

Este resultado entrega una primera estimación de la severidad del riesgo (bajo, moderado, alto, extremo).

2. Ajuste de la Severidad del Riesgo incorporando variables cualitativas adicionales

Para enriquecer la evaluación del riesgo, en este caso, se utilizarán algunas variables cualitativas (5) que reflejan factores de contexto no considerados en el modelo tradicional:

Variable	Descripción
Vulnerabilidad	Grado de exposición o debilidad ante el riesgo.
Velocidad	Tiempo entre el inicio del evento y su impacto.
Interdependencia	Conexión con otros procesos o entidades.
Correlación	Coincidencia o amplificación de riesgos por factores externos.
Impacto en Valor Público	Grado en que el riesgo afecta el mandato, la legitimidad y confianza ciudadana.

Cada variable se califica en una escala de 1 (baja), 2 (media), 3 (alta) y se pondera en este caso al 20% del total. La suma ponderada da un multiplicador cualitativo (entre 1.0 y 3.0) que ajusta el riesgo inherente tradicional, tal como se observa en la siguiente tabla.

Variable	Valor	Porcentaje Ponderación	Subtotal
Vulnerabilidad	(1 - 3)	20%	V × 0.2
Velocidad	(1 - 3)	20%	VE × 0.2
Interdependencia	(1 - 3)	20%	ID × 0.2
Correlación	(1 - 3)	20%	C × 0.2
Impacto en Valor Público	(1 - 3)	20%	VP × 0.2
		Total 100%	**Suma= Multiplicador Cualitativo**

Severidad del Riesgo Ajustada= Severidad del Riesgo Tradicional × Multiplicador Cualitativo

Evaluación de la Exposición al Riesgo

Una vez calculado la Severidad al Riesgo Ajustada, se incorpora la efectividad del control mitigante, usando una escala de 1 (deficiente) a 5 (óptimo). Esto refleja cuánto se reduce el riesgo por los controles mitigantes existentes.

Exposición al Riesgo = Severidad al Riesgo Ajustada ÷ Valor del Control

3. Comparación con el Apetito de Riesgo

El resultado final se clasifica y compara con el umbral institucional definido en la Escala del Apetito de Riesgo, que refleja cuánto riesgo está dispuesta a aceptar la entidad:

Esquema N° 2: Tabla de Exposición al Riesgo y Relación con Apetito de Riesgo

ÍNDICE DE EXPOSICIÓN AL RIESGO	NIVEL DE EXPOSICIÓN AL RIESGO	RELACIÓN CON EL APETITO DE RIESGO
8,0 – 25,0	**NO ACEPTABLE (Na)**	Excede el apetito de riesgo. Requiere intervención inmediata
4,0 – 7,99	**MAYOR (Ma)**	Al límite del apetito de riesgo. Requiere atención prioritaria

3,0 – 3,99	**MEDIA (Md)**	Dentro del apetito de riesgo. Requiere monitoreo periódico
0,2 - 2,99	**MENOR (Me)**	Bien gestionado. Dentro del apetito de riesgo

Caso Práctico: Riesgo en la entrega y pago de subsidios a poblaciones vulnerables

Contexto del riesgo identificado

La entidad pública responsable de la protección social entrega subsidios mensuales a hogares en situación de pobreza extrema. Un proceso crítico es la transferencia oportuna de estos subsidios. Una falla puede tener consecuencias graves para los beneficiarios y para la legitimidad institucional.

Riesgo Crítico: Demoras significativas en el pago de subsidios que pueden afectar gravemente la subsistencia de beneficiarios vulnerables, generando impacto social negativo y cuestionamientos institucionales.

Este riesgo ha sido identificado en el contexto de una auditoría al proceso de gestión y pago de subsidios sociales a población en situación de vulnerabilidad. Se trata de una actividad prioritaria para la política pública y el mandato institucional.

1. Evaluación Tradicional de la Severidad del Riesgo

Variable	Valor	Justificación
Probabilidad	4 (Probable)	Se ha evidenciado un historial de recurrencia de demoras por causas administrativas y técnicas.
Impacto	5 (Catastrófico)	Afecta directamente la subsistencia de los beneficiarios, genera presión política y daño reputacional significativo.

Probabilidad e Impacto: $4 \times 5 = 20 \rightarrow$ Nivel Extremo

2. Evaluación de la Efectividad del Control Clave

- **Descripción del Control:** Validación automatizada semanal del padrón de beneficiarios, con revisión manual ante discrepancias.
- **Diseño del Control:** Preventivo, periódico, semi-automatizado
- **Evaluación del Diseño: del Control: Bueno → Valor = 4**

3. Cálculo de la Exposición al Riesgo

- Severidad del Riesgo ÷ Valor Control Clave Existente: 20 ÷ 4 = 5 → Mayor

Según Escala: Al límite del apetito de riesgo. Requiere atención prioritaria.

4. Evaluación con Ajuste de Severidad y Exposición al Riesgo mediante variables cualitativas adicionales

Análisis y Evaluación de Variables Cualitativas

Variable	Descripción Evaluada	Valor (Escala)	Ponderación	Subtotal
Vulnerabilidad	Beneficiarios sin redes de apoyo ni fuentes alternativas de ingreso	3 (Alta)	0.20	0.60
Velocidad	El efecto negativo es inmediato: en menos de 3 días ya hay impacto social	3 (Alta)	0.20	0.60
Interdependencia	Dependencia de sistemas de otras entidades (registro civil, bancos, etc.)	3 (Alta)	0.20	0.60
Correlación	Riesgo se intensifica con recortes presupuestarios y carga de procesos simultáneos	3 (Alta)	0.20	0.60
Impacto en Valor Público	Afectación del mandato, pérdida de confianza institucional y percepción de abandono estatal	3 (Alta)	0.20	0.60
			100%	3.0

Multiplicador cualitativo = 3.00

Aplicación:

- Nivel de Severidad al Riesgo Ajustado: 20 x 3.0 = 60
- Nivel de Exposición al Riesgo ajustado: 60 ÷ 4 = 15 → **No Aceptable (Na)**

Interpretación: El riesgo supera el Apetito de Riesgo institucional. Requiere intervención inmediata.

Aunque el cálculo tradicional lo ubica en el nivel "**Mayo**r", las condiciones cualitativas elevan la exposición al riesgo al nivel **"No Aceptable"**, superando el nivel de Apetito de Riesgo institucional.

Medidas sugeridas por auditoría interna para tratar el riesgo no aceptable (priorizadas por velocidad)

Variable Relacionada Directamente	Categoría de Medida en Tiempo	Medidas Propuestas
Velocidad	Inmediatas (0–30 días)	Activar protocolo de emergencia para pagos, mesa de crisis, auditoría inmediata
	Corto Plazo (1–3 meses)	Tableros de monitoreo en tiempo real, rediseño del flujo operativo
	Mediano Plazo (3–6 meses)	Indicadores de persistencia y velocidad
Vulnerabilidad	Corto Plazo (1–3 meses)	Validación automatizada del padrón de beneficiarios
	Estratégicas (6–12 meses)	Política transversal de protección del valor público
Interdependencia	Mediano Plazo (3–6 meses)	Alianzas operativas con bancos y registro civil
	Estratégicas (6–12 meses)	Sistemas interoperables, comité de gobernanza de riesgos
Correlación	Mediano Plazo (3–6 meses)	Comité de riesgos críticos, análisis de contextos simultáneos
	Estratégicas (6–12 meses)	Ajustes al plan estratégico de auditoría

Variable Relacionada Directamente	Categoría de Medida en Tiempo	Medidas Propuestas
Impacto en Valor Público	Inmediatas (0–30 días)	Comunicación institucional proactiva con beneficiarios
	Estratégicas (6–12 meses)	Actualización del apetito de riesgo institucional

Justificación de la prioridad

Velocidad Alta = Medidas inmediatas para evitar que el daño se materialice en horas o días.
El resto de las variables cualitativas complementan la exposición, pero si el efecto es inmediato, la contención también debe serlo.

ANEXO Nº 2

CONCEPTOS GENERALES SOBRE APETITO DE RIESGOS Y TOLERANCIA AL RIESGO

Según el glosario de las NOGAI, el Apetito de riesgo corresponde a "*Los tipos y la cantidad de riesgo que la organización está dispuesta a aceptar al perseguir sus estrategias y objetivos."* Es decir, representa el nivel de riesgo que una entidad asume para alcanzar sus objetivos estratégicos, operacionales, financieros y de cumplimiento.

Refleja el nivel de aceptación institucional frente a eventos adversos, considerando su impacto potencial y probabilidad de ocurrencia, y establece el umbral a partir del cual un riesgo se considera inaceptable y requiere una respuesta inmediata, el fortalecimiento de controles u otra acción mitigante.

Por su parte la Tolerancia al Riesgo está definida como las "*Variaciones aceptables en el desempeño con relación al logro de los objetivos*."

Estos conceptos funcionan como referencia clave para:

- La evaluación de la severidad del riesgo o riesgo inherente (combinación de probabilidad e impacto).
- La valoración de la efectividad de los controles mitigantes.
- El cálculo de la exposición al riesgo o riesgo residual.

El auditor interno debe comprender la filosofía de gestión de riesgos utilizada para establecer el apetito y tolerancia al riesgo en la organización, en especial si existe una metodología establecida para determina ambos elementos, y si estos se comunican de manera efectiva por el Jefe de Servicio y los responsables de las áreas operativas.

Lo óptimo es que la organización cuente con una metodología establecida para definir el apetito y la tolerancia al riesgo, ya que las políticas y procedimientos de gestión de riesgos ayudan a garantizar que esta tarea se realice de manera eficaz.

En este contexto, es importante que la función de auditoría interna no asuma responsabilidades de gestión relacionadas con riesgos, tales como es el establecimiento del apetito de riesgo, la tolerancia o la aceptación de responsabilidad general por la gestión de riesgos en nombre de la organización.

Para efecto de esta Guía, el apetito de riesgo se materializa en la escala de clasificación de la exposición al riesgo residual, en la cual se definen los niveles "Menor", "Media", "Mayor" y "No Aceptable", según el siguiente umbral:

Escala del Nivel de Exposición al Riesgo (Ver Anexo N° 5: Tabla Nº 8)

INDICADOR DE EXPOSICIÓN AL RIESGO	ÍNDICE DE EXPOSICIÓN AL RIESGO	NIVEL DE EXPOSICIÓN AL RIESGO	RELACIÓN CON EL APETITO DE RIESGO
NIVEL SEVERIDAD DEL RIESGO ——— **NIVEL EFECTIVIDAD DEL CONTROL**	**8,0 – 25,0**	**NO ACEPTABLE (Na)**	Excede el apetito de riesgo. Requiere intervención inmediata
	4,0 – 7,99	**MAYOR (Ma)**	Al límite del apetito de riesgo. Requiere atención prioritaria
	3,0 – 3,99	**MEDIA (Md)**	Dentro del apetito de riesgo. Requiere monitoreo periódico
	0,2 - 2,99	**MENOR (Me)**	Bien gestionado. Dentro del apetito de riesgo

Ejemplo aplicado del Apetito de Riesgo

Contexto:

Una función de auditoría interna realiza un trabajo al proceso de asignación y pago de subsidios a poblaciones vulnerables. Uno de los riesgos críticos identificados es:

"*Demoras significativas en el pago de subsidios que pueden afectar gravemente la subsistencia de beneficiarios vulnerables, generando impacto social negativo y cuestionamientos institucionales*."

1. Evaluación de la Severidad del Riesgo (riesgo inherente):

- **Probabilidad:** 4 (Probable)
- **Impacto:** 5 (Catastrófico)
- **Severidad del riesgo (Inherente): 4 × 5 = 20 → Nivel Extremo**

Este riesgo se clasifica como extremo, ya que podría comprometer necesidades básicas de la población objetivo, afectando la misión social de la entidad.

2. Evaluación del control clave:

• **Control existente:** Sistema automatizado de calendarización de pagos, con alertas ante retrasos y seguimiento de carga financiera"

• Evaluación de efectividad del control: Regular (2)

(El sistema presenta fallas intermitentes y no cuenta con medidas alternativas de respaldo en casos críticos).

3. Cálculo de la exposición al Riesgo (riesgo residual):

• **Severidad (20) ÷ Efectividad del Control (2) = 10**

4. Comparación con el Apetito y la Tolerancia al Riesgo Institucional:

• Apetito de riesgo definido para este tipo de riesgo: Menor → *Solo se aceptan exposiciones residuales de nivel ≤ 2.99*

• **Tolerancia al riesgo (límite máximo aceptable):** Nivel ≤ *3.99* (como excepción, bajo justificación y monitoreo especial)

5. Interpretación según el Apetito de Riesgo (usando el nivel definido en la Tabla N° 8 del Anexo N° 5):

- **Resultado:** Exposición al Riesgo = 10,0
- **Nivel:** No Aceptable
- **Acción requerida:** La exposición al riesgo residual supera el apetito y la tolerancia al riesgo establecida para este proceso por lo tanto, la entidad debe:

- Reforzar el sistema de alertas con notificaciones en tiempo real y mecanismos de escalamiento automático.
- Establecer controles de respaldo manual para asegurar los pagos en casos de fallas del sistema.
- Mejorar la coordinación interinstitucional (p. ej., con Tesorería y áreas operativas) para garantizar la continuidad operativa del proceso.
- Implementar un monitoreo continuo del cumplimiento de plazos críticos, con reportes periódicos al Jefe de Servicio.

ANEXO Nº 3

MODELO DE MADUREZ DEL PROCESO DE GESTIÓN DE RIESGOS

El presente Anexo establece el Modelo de Madurez del Proceso de Gestión de Riesgos, cuyo propósito es evaluar el nivel de desarrollo, integración y efectividad del Sistema de Gestión de Riesgos, promoviendo un enfoque evolutivo, preventivo y de mejora continua.

Este modelo constituye un instrumento estructural del sistema, en concordancia con los principios de gobernanza, supervisión y responsabilidad directiva establecidos en la GGSAI N°3.

1. Objetivo del Modelo

El Modelo de Madurez tiene por finalidad:

a) Determinar el nivel de integración del riesgo en la planificación estratégica.
b) Evaluar el grado de institucionalización del proceso de gestión de riesgos.
c) Medir la efectividad de los mecanismos de control asociados.
d) Servir como insumo formal para la asesoría técnica del CAIGG.
e) Fundamentar planes de fortalecimiento institucional.
f) Contribuir a la rendición de cuentas en materia de gestión de riesgos.

La evaluación tendrá carácter anual y será reportada conforme al mecanismo establecido en este Documento Técnico.

2. Estructura del Modelo

El Modelo de Madurez se estructura en:

- Cinco niveles progresivos
- Dimensiones evaluativas
- Criterios objetivos de verificación
- Escala de puntuación
- Mecanismo formal de reporte

3. Niveles de Madurez

El sistema se evaluará conforme a los siguientes niveles:

Nivel 1 – Inicial (Reactivo)

Características:

- La gestión de riesgos no está formalmente estructurada.
- Existen acciones aisladas y no sistemáticas.
- No hay integración con planificación estratégica.
- La gestión es predominantemente correctiva.
- No existen métricas formales.

Riesgo institucional alto por baja capacidad preventiva.

Nivel 2 – Básico (Formalización incipiente)

Características:

- Existe política o lineamientos formales.
- Se realizan matrices de riesgo, pero de forma parcial.
- Limitada participación de la alta dirección.
- Integración incipiente con control interno.
- Escasa trazabilidad documental.

El sistema opera, pero no está completamente integrado.

Nivel 3 – Intermedio (Integrado)

Características:

- Gestión de riesgos formalizada y documentada.
- Integración con planificación estratégica y operativa.
- Matrices actualizadas periódicamente.
- Evaluación de riesgo residual.
- Reportabilidad estructurada a la dirección.

El sistema comienza a influir en la toma de decisiones.

Nivel 4 – Avanzado (Gestionado estratégicamente)

Características:

- El riesgo es considerado en decisiones estratégicas.
- Existe apetito y tolerancia al riesgo definidos.
- Indicadores de gestión de riesgos implementados.
- Integración con auditoría interna.
- Gestión prospectiva de riesgos emergentes.

El riesgo forma parte del modelo de gobernanza.

Nivel 5 – Optimizado (Cultura institucional)

Características:

- Gestión de riesgos integrada en toda la organización.
- Cultura preventiva instalada.
- Evaluación sistemática de riesgos de probidad.
- Uso de analítica y monitoreo continuo.
- Mejora continua basada en resultados y lecciones aprendidas.

El riesgo es un habilitador estratégico del valor público.

4. Dimensiones de Evaluación

La evaluación considerará al menos las siguientes dimensiones:

a. Gobernanza y liderazgo
b. Marco normativo interno
c. Integración estratégica
d. Metodología aplicada
e. Gestión de riesgos de probidad
f. Seguimiento y monitoreo
g. Cultura organizacional

Cada dimensión será evaluada en una escala de 1 a 5 conforme a los niveles definidos.

5. Metodología de Evaluación

5.1. Escala de Puntuación

Cada dimensión se evaluará conforme a:

Puntaje	Nivel de Madurez
1	Inicial
2	Básico
3	Intermedio
4	Avanzado
5	Optimizado

La puntuación global corresponderá al promedio ponderado de las dimensiones evaluadas.

5.2. Evidencia Requerida

La evaluación deberá sustentarse en:

- Política de Riesgos formal aprobada
- Matriz institucional actualizada
- Informe de aseguramiento
- Reportes de seguimiento
- Planes de Tratamientos
- Evidencia de integración con planificación

No son válidas las evaluaciones basadas únicamente en declaración.

6. Integración con la Gestión de Riesgos de Probidad

El modelo incorporará explícitamente la evaluación de:

- Identificación sistemática de riesgos de probidad.
- Tratamiento preventivo.
- Señales de alerta estructuradas.
- Evaluación de riesgos emergentes.
- Medidas sistémicas y no solo sancionatorias.

El riesgo de probidad constituye dimensión obligatoria del modelo.

7. Reporte Anual

El resultado de la evaluación deberá:

a) Ser aprobado por la autoridad superior del servicio.
b) Ser informado al CAIGG conforme al mecanismo definido.
c) Incluir plan de fortalecimiento cuando el nivel sea ≤ 3.
d) Incorporarse como antecedente para la planificación de auditoría interna.

Los formatos de reporte serán entregados por el CAIGG en la respectiva página web y actualizados anualmente.

ANEXO Nº 4

PASOS PARA DEFINIR UN OBJETIVO

Un objetivo debe ser claro, específico y medible para que pueda guiar las acciones necesarias para su cumplimiento

1. Identificar el Propósito: Entiende la razón detrás del objetivo. ¿Qué se espera lograr? ¿Por qué es importante?

2. Ser Específico: Define claramente lo que se quiere lograr. Evita generalidades.

3. Medible: Asegúrate de que el objetivo puede ser evaluado mediante métricas o indicadores específicos.

4. Alcanzable: El objetivo debe ser realista y posible de lograr con los recursos disponibles.

5. Relevante: Debe estar alineado con los valores, misión y visión de la organización o proyecto.

6. Tiempo: Especifica un marco temporal en el cual se espera cumplir el objetivo.

Redacción de un objetivo

Para redactar un objetivo siguiendo el formato SMART (Específico, Medible, Alcanzable, Relevante y con un Tiempo definido), puedes utilizar la siguiente estructura:

1. Quién: Indica quién es responsable.
2. Qué: Describe qué se va a lograr.
3. Cuando: Define el plazo para lograrlo.
4. Dónde: Si aplica, especifica el lugar.
5. Por qué: Menciona el propósito o la razón detrás del objetivo.
6. Cómo: Explica brevemente cómo se logrará.

Ejemplo de Redacción de un objetivo:

Objetivo: Incrementar las ventas trimestrales en un 10% para el final del T3 de 2025 en el mercado regional mediante la implementación de nuevas estrategias de marketing digital.

Responde a las siguientes interrogantes:

Quién:

El equipo de ventas y marketing.

Qué:

Incrementar las ventas trimestrales.

Cuando:

Para el final del T3 de 2025.

Dónde:
En el mercado regional.

Por qué:
Para mejorar la participación en el mercado y aumentar los ingresos.

Cómo:
Implementando nuevas estrategias de marketing digital.

Formato SMART del Ejemplo:

Específico:
Incrementar las ventas trimestrales.

Medible:
En un 10%.

Alcanzable:
Mediante estrategias de marketing digital.

Relevante:
Para mejorar la participación en el mercado y aumentar los ingresos.

Tiempo:
Para el final del T3 de 2025.

ANEXO Nº 5

GUÍA BÁSICA PARA EL LEVANTAMIENTO DE INFORMACIÓN DE LOS PROCESOS Y MODELAMIENTO DE RIESGOS[16]

Con el fin de entregar una guía elemental para mejor comprender la estructura de los procesos críticos de la organización gubernamental y la identificación de éstos, sus subprocesos y etapas, es posible señalar que un proceso, como concepto, es un conjunto de actividades, tareas, eventos y responsabilidades que se realizan o suceden con un determinado fin, que recibe uno o más insumos o pasos (inputs) y crea un producto de valor para otro usuario o cliente, formando una cadena orientada a obtener un resultado final (outputs). De su diseño y documentación depende el éxito de la gestión en la organización.

Por consiguiente, podemos identificar que los elementos básicos de un proceso son:

- Existencia de un objetivo para el proceso.
- La existencia de un conjunto de actividades, tareas, eventos y responsabilidades.
- Todas ellas se realizan con un determinado fin.
- Reciben uno o más insumos, pasos o inputs.
- Crean un producto de valor para otro usuario o cliente.
- Forman una cadena orientada a obtener un resultado final u output.

Para realizar un adecuado análisis es necesario identificar y describir detalladamente, al mayor nivel posible, como se conforman los procesos en la institución.

Un proceso puede descomponerse en un número determinado de subprocesos que se relacionan en que los outputs de unos son los inputs de los siguientes, hasta que el último subproceso genera como output el producto o servicio final del proceso.

En todo caso, perfectamente podrían existir procesos críticos en que, por su naturaleza y características particulares, no sea posible desagregarlos en subprocesos. En estos casos, el análisis se debe realizar en razón de las etapas que componen el proceso, ya que este corresponde al mayor nivel de detalle posible de desagregación.

Las etapas son las principales fases que componen un subproceso o proceso. Éstas se conforman por una serie de actividades que se realizan con la finalidad de lograr el objetivo perseguido en la etapa y que está directamente relacionado con los objetivos de los subprocesos y el proceso.

El mecanismo de análisis recomendado por este Consejo de Auditoría considera, en primer lugar, identificar y comprender, entre otros, los siguientes elementos en cada proceso crítico (Información obtenida de la Fase Genérica: Obtención de Información de la organización gubernamental y del Contexto Externo y de la Fase Genérica: Comprensión de los Procesos de la organización y del Contexto Externo):

[16] Se recomienda leer en forma complementaria, el Documento Técnico sobre metodologías para el levantamiento y modelamiento de procesos, publicado por el Consejo de Auditoría.

- El tipo de proceso; estratégico o de soporte.
- Él o los responsables de la gestión.
- Determinar si existen subprocesos y cuáles son las etapas que lo componen.
- Determinar las actividades que conforman las etapas.
- El inicio y fin de cada proceso, subproceso y etapa.
- Las personas implicadas que desarrollan el conjunto de actividades, tareas y eventos.
- El objetivo o misión del proceso, subprocesos y etapas.
- Las entradas o recursos requeridos y los requisitos de calidad de los subprocesos y procesos.
- Las salidas o resultados esperados y los requisitos de calidad de los subprocesos y procesos.
- Los clientes y sus requerimientos (valoración de las salidas).
- Los proveedores y los requerimientos.
- Los controles existentes para las entradas y actividades desarrolladas en cada etapa.
- La documentación de apoyo.
- Los registros que se generan y que se analizan.
- Los indicadores de desempeño que existen para partes o para el total del proceso (de eficacia y/o eficiencia).
- Las metas asociadas a la gestión en los procesos.

Especial atención debe darse al objetivo operativo de cada etapa, es decir, cual es la finalidad que ésta tiene en la consecución de la salida o producto del subproceso o proceso, según corresponda.

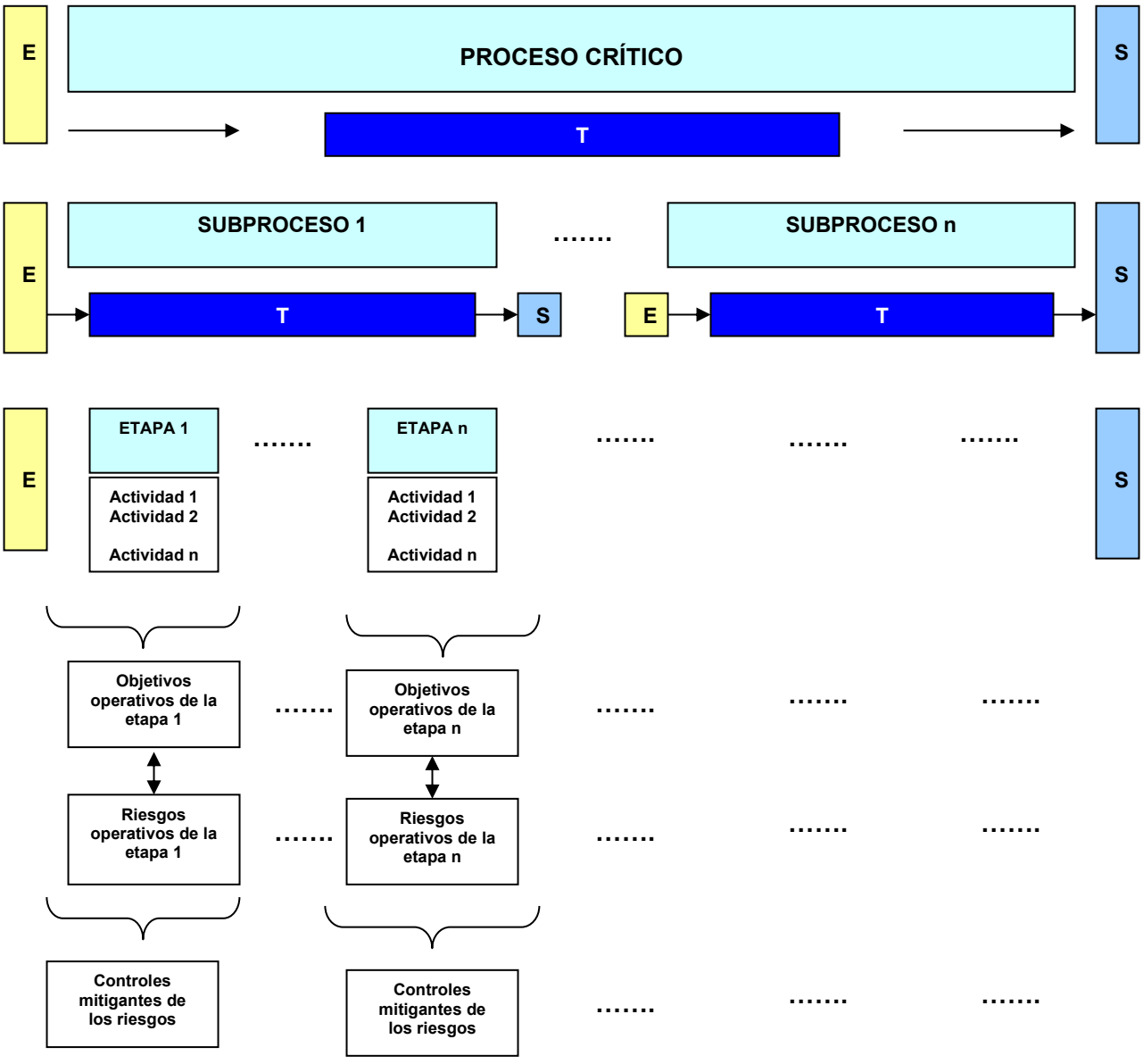
Posteriormente, se deben identificar todos los eventos que podrían afectar negativamente la consecución del objetivo operativo de cada etapa. Este aspecto es recomendable analizarlo desde el punto de vista de cómo afectan a dicho objetivo, las amenazas, errores o deficiencias de las entradas al subproceso o proceso en cada etapa, especialmente, en la etapa que comienza a ejecutarse un subproceso o proceso y, cómo afectan estas mismas variables, a las actividades o tareas de gestión y control realizadas en el desarrollo de cada etapa.

Para efecto de este análisis, las actividades desarrolladas en la etapa también consideran en forma implícita las tareas necesarias para producir y controlar las salidas del subproceso o proceso.

Este tipo de análisis tiene como principal finalidad, identificar donde se encuentran, al mayor nivel de detalle posible, en un determinado proceso, los puntos críticos que deben ser evaluados y controlados, respecto del nivel de severidad y/o exposición que presentan los riesgos que se han identificado en el estudio realizado.

Para efecto de una mejor comprensión de lo previamente señalado, se presenta un esquema explicativo a continuación:

Esquema Gráfico para Desagregación y Análisis de Procesos Críticos



E Entrada o inputs: Recursos necesarios para producir la salida.

T Transformación: Tareas, actividades y responsabilidades.

S Salidas u outputs: Producto, servicio y finalidad del subproceso o proceso.

ANEXO Nº 6

EJEMPLO: MODELO DE POLÍTICA DE GESTIÓN DE RIESGOS

El Servicio xxxxx xxx adopta la presente Política de Gestión de Riesgos como instrumento estructural del Sistema de Control Interno, en conformidad con el Documento Técnico N°70 del Consejo de Auditoría Interna General de Gobierno (CAIGG).

El Proceso de Gestión de Riesgos Institucional tiene por finalidad identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, operacionales y de cumplimiento, asegurando su integración en la planificación institucional y en la toma de decisiones.

La gestión del riesgo constituye un proceso permanente, sistemático y transversal a todos los procesos institucionales.

1. Alcance

El Proceso de Gestión de Riesgos Institucional será aplicable a:

- Procesos estratégicos.
- Procesos misionales.
- Procesos de soporte.
- Programas, proyectos e iniciativas institucionales.
- Riesgos emergentes derivados del entorno externo.

Se incorporarán de manera transversal los:

- Riesgos estratégicos.
- Riesgos operacionales.
- Riesgos financieros.
- Riesgos tecnológicos.
- Riesgos de cumplimiento normativo.
- Riesgos de probidad administrativa.
- Riesgos reputacionales.
- Riesgos emergentes.

Los riesgos de probidad administrativa deberán incorporarse conforme a lo establecido en el capítulo específico del DT 70, asegurando su trazabilidad y tratamiento sistemático.

2. Principios Rectores

El Proceso de Gestión de Riesgos Institucional se regirá por los siguientes principios:

- Enfoque preventivo y prospectivo.
- Integración en la planificación estratégica.
- Responsabilidad directiva.
- Mejora continua.
- Tolerancia mínima frente a riesgos de probidad.

3. Apetito de Riesgo y Tolerancia al Riesgo

3.1 Apetito de Riesgo Institucional

El Apetito de Riesgo corresponde al nivel global de exposición al riesgo que la Máxima Autoridad Institucional está dispuesta a aceptar para el logro de los objetivos estratégicos.

El Apetito de Riesgo será determinado considerando:

- La misión institucional.
- Las prioridades gubernamentales.
- El contexto externo.
- El nivel de madurez del sistema de control interno.
- La capacidad de respuesta organizacional.

El Apetito de Riesgo se expresará mediante:

- Rangos de Nivel de Exposición al Riesgo aceptable en la Matriz de Riesgos Institucional.
- Declaraciones cualitativas diferenciadas por tipo de riesgo.
- Umbrales máximos permitidos de riesgo residual.

Como criterio general:

Podrá aceptarse un mayor nivel de exposición en riesgos asociados a innovación y mejora de servicios públicos.

No se aceptará exposición significativa en riesgos de probidad administrativa, fraude, corrupción o incumplimiento legal.

3.2 Tolerancia al Riesgo

La Tolerancia al Riesgo corresponde a los límites específicos de variaciones aceptables en el desempeño con relación al logro de los objetivos.

Para cada riesgo priorizado se definirán umbrales que determinen:

- Zona dentro del apetito.
- Zona de advertencia.
- Zona fuera de tolerancia.

Cuando el Riesgo Residual supere el nivel de tolerancia definido:

- Deberá implementarse obligatoriamente un plan de tratamiento.
- Se informará a la autoridad superior.
- Se evaluará la necesidad de fortalecer controles o rediseñar procesos.

En materia de riesgos de probidad administrativa, la tolerancia será mínima o nula cuando el riesgo comprometa el principio de probidad administrativa o la legalidad.

4. Metodología

El Proceso de Gestión de Riesgos Institucional se desarrollará conforme al ciclo establecido en el DT N°70.

5. Estrategias de Tratamiento

El tratamiento del riesgo podrá considerar:

- Evitar el riesgo.
- Reducir la probabilidad.
- Reducir el impacto.
- Fortalecer controles existentes.
- Implementar nuevos controles.
- Transferir o compartir el riesgo.
- Aceptar el riesgo dentro de los límites definidos de apetito y tolerancia.

Toda decisión de aceptación de riesgos significativos deberá quedar debidamente fundada y documentada.

6. Roles y Responsabilidades

Jefe de Servicio

- Aprobar la Política de Gestión de Riesgos.
- Definir el Apetito de Riesgo.
- Supervisar el cumplimiento del proceso.

Directivos

- Integrar la gestión de riesgos en la planificación.
- Asegurar la implementación de controles.

Responsables de Proceso

- Identificar y evaluar riesgos.
- Proponer tratamientos.
- Reportar desviaciones.

Auditoría Interna

- Evaluar la efectividad del Proceso de Gestión de Riesgos.
- Emitir recomendaciones.
- No asumir funciones de gestión operativa.

7. Monitoreo y Evaluación

El Proceso de Gestión de Riesgos Institucional será objeto de:

- Seguimiento periódico.
- Actualización anual de la Matriz de Riesgos.
- Evaluación del Nivel de Madurez del sistema, conforme al modelo establecido en el DT 70.
- Reporte a la autoridad superior y al CAIGG.

8. Declaración Final

La Gestión de Riesgos Institucional no constituye un ejercicio formal o documental, sino un componente estructural de la gobernanza pública.

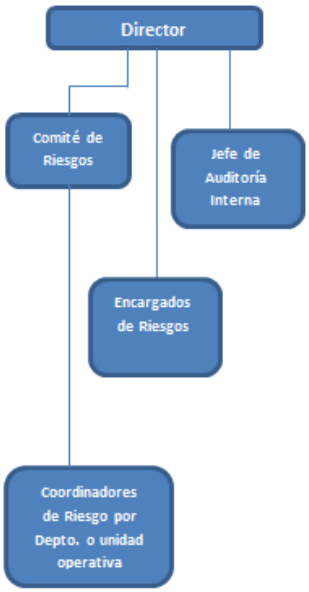
El riesgo debe ser gestionado de manera consciente, sistemática y alineada con el Apetito de Riesgo definido por la autoridad.

La probidad administrativa se protege fortaleciendo el sistema de control interno y no exclusivamente reaccionando frente al evento adverso.

ANEXO Nº 7

EJEMPLOS DE MODELOS DE DEFINICIÓN DE ROLES Y RESPONSABILIDADES

EJEMPLO 1

Ejemplo de Estructura Organizacional	Responsabilidades de Administración de Riesgos	Ejemplo de Roles Claves	Ejemplo de Tareas
		Rol Supervisor Coordinar decisión	**Director:** • Aprobación de políticas escritas • Evaluar efectividad esquema de gestión de riesgos **Comité de Riesgos:** • Supervisar y revisar implementación del marco de gestión de riesgos • Monitorear perfil de riesgo de la organización • Asegurarse que los riesgos han sido considerados en planes de largo plazo
		Comprensión del riesgo	**Encargado de Riesgos:** • Definir prioridades de riesgo • Arbitrar y resolver conflictos • Alienar respuesta al riesgo a todas las estrategias de la organización y objetivos del negocio • Monitorear el avance general de la implementación de las estrategias de tratamiento
		Operación y soporte Administrar y reportar riesgos a nivel de negocios	**Coordinadores de Riesgo:** • Alinear a través de la organización las prioridades y estrategias de identificación de riesgos • Medición de impacto de los riesgos • Formular respuestas apropiadas al riesgo • Mejoras continua de mediciones y procesos • Monitorear el avance en su área de la implementación de las estrategias de tratamiento
		Revisión cumplimiento de riesgos específicos	**Auditor Interno:** • Revisión del cumplimiento de riesgos específicos, fraude, oportunidad de negocios, seguros, etc. • Reportes al Director
		Recolectar, analizar y reportar riesgos y respuestas a los riesgos en forma independiente y a través de auditoría interna	**Unidad de Auditoría Interna:** • Comunicar y reforzar políticas de medición y monitoreo • Revisión de cumplimiento • Revisión de cumplimiento del monitoreo • Reportes al Director

EJEMPLO 2

Roles Claves	Responsables	Tareas y Actividades
SUPERVISOR Y COORDINACION DE DECISIONES	Jefe de Servicio	Definir el Apetito de Riesgo y Tolerancia al Riesgo para la institución y para las áreas operacionales. Aprobar y formalizar la política de gestión de riesgos y el procedimiento para la elaboración de los documentos que surjan del desarrollo de cada fase del proceso de gestión de riesgos, aprobado por el Comité de Riesgos. Remitir a los centros de responsabilidad respectivos, el plan de comunicación y consulta, por el cual se entregan las orientaciones del trabajo a realizar durante el periodo. Tomar conocimiento del avance de cada estrategia de mitigación y solicitar al Comité de Riesgos las acciones que se requieran para su cumplimiento, a partir del informe de monitoreo de estrategias elaborado por la Coordinación de Riesgos, revisado y aprobado por el Comité. Conocer y aprobar las estrategias que se emplearán para tratar los riesgos priorizados y rankeados por el Comité. Asegurar la incorporación mecanismos de identificación prospectiva respecto de los riesgos emergentes. Adoptar decisiones estratégicas cuando un riesgo emergente pueda afectar los objetivos institucionales. Remitir por oficio al CAIGG los reportes del proceso de gestión de riesgos en el Ministerio según las instrucciones que correspondan.

Roles Claves	**Responsables**	**Tareas y Actividades**
	Comité de Riesgos	Proponer alternativas para la definición del Apetito de Riesgo para el Jefe de Servicio. Revisar la implementación del proceso de gestión anual de riesgos. Revisar las propuestas enviadas por la coordinación de riesgos del Servicio, y revisar y aprobar los documentos de cada fase del proceso de gestión de riesgos. Participar en las instancias convocadas por la coordinación de riesgos. Aprobar las estrategias de mitigación de los riesgos priorizados, asegurándose de que los riesgos de mayor exposición incluidos en el ranking anual hayan sido considerados en planes de tratamiento. Conocer y aprobar cada uno de los reportes anuales del monitoreo de las estrategias de mitigación incluidas en el plan de tratamiento.
COMPRENSIÓN DEL RIESGO	Coordinación de Riesgos	Planificar y coordinar el proceso anual de gestión de riesgos. Coordinar el levantamiento, consolidación y monitoreo de riesgos emergentes. Asesorar técnicamente a los centros de responsabilidad respecto de cada fase de implementación del proceso de gestión de riesgos. Proponer al comité de riesgos los documentos que dan cumplimiento a las distintas fases del proceso para su aprobación y posterior entrega al Jefe de Servicio. Elaborar los reportes de monitoreo del plan de tratamiento de riesgos para la aprobación del Comité.
ADMINISTRAR Y REPORTAR RIESGOS A NIVEL INSTITUCIONAL	Jefaturas y contrapartes designadas para integrar el Comité De Riesgos	Elaborar propuesta de matrices de riesgos que contengan un levantamiento de procesos, la evaluación de riesgos y la descripción de los controles de mitigación de cada uno de ellos. Monitorear cambios regulatorios, tecnológicos, sociales o presupuestarios. Incorporar análisis prospectivo en la planificación. Activar evaluación cuando detecten señales tempranas.

Roles Claves	**Responsables**	**Tareas y Actividades**
		Establecer propuestas de planes de tratamiento de riesgos y señales de alerta de los riesgos priorizados. Contribuir a la mejora continua de mediciones y procesos. Monitorear y reportar los grados de avance en su área respecto a la implementación de las estrategias de tratamiento. Elaborar nuevos planes de tratamiento frente a estrategias cuya probabilidad de implementación no sea posible, para posterior aprobación del Comité. Incorporar las recomendaciones efectuadas por la Coordinación de Riesgos y el Comité de Riesgos. Participar de las convocatorias realizadas por la Coordinación de Riesgos.
ANALIZAR Y REPORTAR	Función de Auditoría Interna	Realizar actividades de aseguramiento y/o consultoría al Proceso de Gestión de Riesgos, estableciendo hallazgos y recomendaciones e identificando oportunidades de mejora del proceso. Evaluar si la entidad está identificando adecuadamente los riesgos emergentes. Puede emitir recomendaciones en aspectos de riesgos emergentes. Puede advertir sobre riesgos no considerados en la matriz de riesgos.

ANEXO Nº 8

ROL DE LA AUDITORÍA INTERNA EN EL PROCESO DE GESTIÓN DE RIESGOS EN EL SECTOR GUBERNAMENTAL

Cuando nos encontramos en una entidad gubernamental que cuenta con un Proceso de Gestión de Riesgos en operación; la formulación de Matriz de Riesgos y las estrategias para tratar y monitorear los riesgos pasan a ser parte de los elementos que la auditoría interna siempre debe considerar en su planificación y programación.

Por lo tanto, en base a normas de auditoría interna[17] y en la experiencia que se ha obtenido en el levantamiento de riesgos en el Sector Gubernamental, se puede concluir que el rol fundamental de la auditoría interna en el Proceso de Gestión de Riesgos será proveer aseguramiento objetivo a la dirección sobre la efectividad de las actividades del proceso de gestión de riesgos para ayudar a asegurar que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente.

En las organizaciones se debe comprender que la Jefatura Superior siempre mantiene la responsabilidad de la gestión de riesgo y que los auditores internos deben proveer asesoría, y motivar las decisiones gerenciales sobre riesgos, y no tomar decisiones sobre gestión de riesgo.

Estas directrices[18] deben afectar en forma gradual el enfoque y las orientaciones con las que en la actualidad se definen las actividades de auditoría:

1.- Roles para la auditoría interna en el Proceso de Gestión de Riesgos en el Sector Gubernamental

Los principales factores que los auditores internos deben tomar en cuenta cuando determinen el rol de auditoría interna son si la actividad representa alguna amenaza sobre la independencia y objetividad al realizar su trabajo, y si podría mejorar los Procesos de Gestión de Riesgo y el control interno en la organización.

1.1.- Principales Roles recomendados en el Proceso de Gestión de Riesgos en el Sector Gubernamental

- Realizar evaluación y entregar aseguramiento sobre el Proceso de Gestión de Riesgo a la dirección.
- Brindar aseguramiento de que los riesgos son correctamente evaluados en el Proceso de Gestión de Riesgos.
- Evaluar los procesos de gestión de riesgos.
- Revisión del manejo y evaluación de reportes de riesgos claves.
- Evaluar la elaboración de informes sobre los riesgos clave.
- Revisar la gestión de riesgos clave.

[17] Normas Globales de Auditoría Interna – Instituto de Auditores Internos - THEIIA.
[18] Adaptado de The Role of Internal Auditing in Enterprise-wide Risk Management, January 2009 – THEIIA.

1.2.- Algunos Roles que deben realizarse con independencia y objetividad en el Proceso de Gestión de Riesgos en el Sector Gubernamental

- Facilitación, identificación y evaluación de riesgos.
- Entrenamiento a la alta dirección sobre respuesta a riesgos.
- Coordinación de actividades del Proceso de Gestión de Riesgos.
- Mantenimiento y desarrollo del marco del Proceso de Gestión de Riesgos.
- Defender el establecimiento del Proceso de Gestión de Riesgos.
- Desarrollo de estrategias de gestión de riesgo para aprobación de Jefatura de la organización gubernamental.
- Asesorar a la dirección para responder a los riesgos.
- Coordinar actividades del Proceso de Gestión de Riesgos.
- Consolidar la elaboración de informes sobre riesgos.

2.- Algunos Roles que auditoría interna NO deben realizar en el Proceso de Gestión de Riesgos en el Sector Gubernamental

- Establecer el nivel de Riesgo Aceptado.
- Imponer Procesos de Gestión de Riesgos.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos.
- Tener roles y responsabilidad de la gestión de los riesgos.

ANEXO Nº 9

CRITERIOS: TABLAS DE VALUACIÓN PARA CONSTRUIR LA MATRIZ DE RIESGOS

1.- SEVERIDAD DEL RIESGO

1.1.- Cuadro Nº 1: Categorías de Probabilidad:

Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

1.2.- Cuadro Nº 2: Categorías de Impacto:

Categoría	Valor	Descripción
Catastróficas	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización y del Gobierno. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal en el año en curso.
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización y del Gobierno. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

1.3.- Cuadro Nº 3: Nivel de Severidad del Riesgo:

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)
Casi Certeza (5)	Mayores (4)	EXTREMO (20)
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)
Casi Certeza (5)	Menores (2)	ALTO (10)
Casi Certeza (5)	Insignificantes (1)	ALTO (5)
Probable (4)	Catastróficas (5)	EXTREMO (20)
Probable (4)	Mayores (4)	EXTREMO (16)
Probable (4)	Moderadas (3)	ALTO (12)
Probable (4)	Menores (2)	ALTO (8)
Probable (4)	Insignificantes (1)	MODERADO (4)
Moderado (3)	Catastróficas (5)	EXTREMO (15)
Moderado (3)	Mayores (4)	EXTREMO (12)
Moderado (3)	Moderadas (3)	ALTO (9)
Moderado (3)	Menores (2)	MODERADO (6)
Moderado (3)	Insignificantes (1)	BAJO (3)
Improbable (2)	Catastróficas (5)	EXTREMO (10)
Improbable (2)	Mayores (4)	ALTO (8)
Improbable (2)	Moderadas (3)	MODERADO (6)
Improbable (2)	Menores (2)	BAJO (4)
Improbable (2)	Insignificantes (1)	BAJO (2)
muy improbable (1)	Catastróficas (5)	ALTO (5)
muy improbable (1)	Mayores (4)	ALTO (4)
muy improbable (1)	Moderadas (3)	MODERADO (3)
muy improbable (1)	Menores (2)	BAJO (2)
muy improbable (1)	Insignificantes (1)	BAJO (1)

En el cuadro anterior se muestra el resultado de la combinación entre las categorías del nivel de impacto del riesgo y las categorías del nivel de probabilidad de ocurrencia del riesgo, es decir, el nivel de severidad.

De ese esquema se puede observar que las categorías de impacto tienen una mayor incidencia en el nivel de severidad asignado, puesto que aunque la probabilidad de ocurrencia sea menor, al tratarse de riesgos con impactos altos, cualquier materialización del riesgo (aunque sea en sólo una oportunidad) tendrá una consecuencia significativa en el uso de los recursos y en el cumplimiento de los objetivos del proceso examinado.

Esto explica los casos en que a igual valor, la severidad del riesgo es distinta. A modo de ejemplo se presentan en el **Cuadro N° 4**, las siguientes relaciones:

- Cuadro Nº 4: Ejemplo de casos con distinta Severidad del Riesgo:

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
muy improbable (1)	Mayores (4)	ALTO (4)
Probable (4)	Insignificantes (1)	MODERADO (4)

Probable	**(4)**	**Moderadas**	**(3)**	**ALTO (12)**
Moderado	**(3)**	**Mayores**	**(4)**	**EXTREMO (12)**

2.- CLASIFICACIÓN DEL CONTROL CLAVE

2.1.- Diseño del control

- **Cuadro Nº 5: Oportunidad de la Aplicación del Control (O):**

Clasificación	Descripción
Preventivo (Pv)	Controles claves que actúan antes o al inicio de una actividad.
Correctivo (Cr)	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias.
Detectivo (Dt)	Controles claves que sólo actúan una vez que el proceso ha terminado.

- **Cuadro Nº 6: Periodicidad en la Aplicación del Control (PD):**

Clasificación	Descripción
Permanente (Pe)	Controles claves aplicados durante todo el proceso, es decir, en cada operación.
Periódico (Pd)	Controles claves aplicados en forma constante sólo cuando ha transcurrido un período específico de tiempo.
Ocasional (Oc)	Controles claves que se aplican sólo en forma ocasional en un proceso.

- **Cuadro Nº 7: Automatización en la Aplicación del Control (A):**

Clasificación	Descripción
100% automatizado (At)	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas informatizados.
Semi – automatizado (Sa)	Controles claves incorporados en el proceso, cuya aplicación es parcialmente desarrollada mediante sistemas informatizados.
Manual (Ma)	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados.

2.2.- Cuadro Nº 8: Escala de Clasificación de la Efectividad de los Controles

CUMPLIMIENTO CON NORMAS O REQUISITOS DE CONTROL	CARACTERÍSTICAS DISEÑO CONTROL CLAVE/FUNDAMENTAL			CLASIFICACIÓN	VALOR DEL DISEÑO DEL CONTROL
	PERIODICIDAD (PD)	OPORTUNIDAD (O)	AUTOMATIZACIÓN (A)		
CUMPLIMIENTO ADECUADO	PERMANENTE	PREVENTIVO	INFORMATIZADO	OPTIMO	5
CUMPLIMIENTO ADECUADO	PERMANENTE	CORRECTIVO	INFORMATIZADO		
CUMPLIMIENTO ADECUADO	PERMANENTE	DETECTIVO	INFORMATIZADO	BUENO	4
CUMPLIMIENTO ADECUADO	PERIODICO	PREVENTIVO	SEMI INFORMAT		
CUMPLIMIENTO ADECUADO	PERIODICO	CORRECTIVO	SEMI INFORMAT	*MAS QUE REGULAR*	3
CUMPLIMIENTO ADECUADO	PERIODICO	DETECTIVO	SEMI INFORMAT		
CUMPLIMIENTO ADECUADO	OCASIONAL	PREVENTIVO	MANUAL	REGULAR	2
CUMPLIMIENTO ADECUADO	OCASIONAL	CORRECTIVO	MANUAL		
CUMPLIMIENTO ADECUADO	OCASIONAL	DETECTIVO	MANUAL	DEFICIENTE	1
INSUFICIENTE	NO DETERMINADO	NO DETERMINADO	NO DETERMINADO	INEXISTENTE	1

Para examinar un control, en primer lugar, debe expresarse con un breve detalle de las actividades de control realizadas, analizando su nivel de documentación y segregación de funciones (quién autoriza o revisa debe ser distinta a quién ejecuta). Hay que relevar que el control debe expresarse claramente, señalando qué se hace, cómo se hace, quién lo hace y cuándo lo realiza. Una vez definido, se debe evaluar si el control mitigante asociado a un riesgo tiene un nivel de cumplimiento adecuado respecto de los requisitos de control básicos que en este modelo se han relevado para dar razonable seguridad de cumplimiento de los objetivos y metas. Esto implica realizar un análisis integral de los referidos requisitos (segregación, autorización, formalización, etc.) y determinar si éstas se cumplen de para un control examinado en particular.

Producto de este análisis, se puede dar que los referidos requisitos se cumplan satisfactoriamente, es decir, que el control esté sustentado en una estructura básica sólida. Posteriormente, se debe seguir con el análisis del diseño del control, este aspecto es relevante, ya que los riesgos son por naturaleza dinámicos y requieren que los controles tengan una estructura que se oriente a la prevención de la materialización del efecto de los riesgos dinámicos.

Finalmente, se debe clasificar el nivel de efectividad del control examinado, de acuerdo con el esquema presentado, asignándole el valor respectivo según la escala.

En caso de que esto no ocurra, es decir, los requisitos no presentan un cumplimiento suficiente en el control examinado, debe entenderse que su nivel de cumplimiento es insuficiente y corresponde clasificarlo como si se tratara de un control inexistente, con valoración de 1, sin que ya sea necesario evaluar la efectividad en el diseño del control respecto de la ocurrencia del riesgo.

Por consiguiente, debe clasificarse como inexistente, con nivel de eficiencia del control examinado de 1, de acuerdo con la escala contenida en el esquema presentado.

Para ver mayores detalles de los requisitos de control adecuado considerados en este modelo ver **Anexo Nº 15**.

Al describir los controles existentes, se debe señalar al menos: la norma o guía que lo instruye, quién lo realiza, qué actividades desarrolla, cómo las ejecuta y cuándo y cómo se evidencia su cumplimiento (registros documentales o electrónicos en el sistema).

3.- NIVELES DE CLASIFICACIÓN DEL NIVEL DE EXPOSICIÓN AL RIESGO

La exposición al riesgo está determinada por la severidad del riesgo dividida por la eficiencia del control asociado a ese riesgo. Estos elementos se obtienen de las relaciones detalladas previamente en este anexo. A continuación, se presenta la escala de nivel de exposición al riesgo que los califica:

Cuadro Nº 9: Escala del Nivel de Exposición al Riesgo

INDICADOR DE EXPOSICIÓN AL RIESGO	VALOR	NIVEL DE EXPOSICIÓN AL RIESGO
NIVEL SEVERIDAD DEL RIESGO / NIVEL EFICIENCIA DEL CONTROL	8,0 – 25,0	NO ACEPTABLE (Na)
	4,0 – 7,99	MAYOR (Ma)
	3,0 – 3,99	MEDIA (Md)
	0,2 - 2,99	MENOR (Me)

Tal como se señaló, la escala previamente presentada, ha sido construida en base a la relación entre el nivel de severidad del riesgo (Bajo, Moderado, Alto. Extremo) y el nivel de eficiencia del control asociado a ese riesgo (Deficiente, Regular, Más que regular, Bueno, Óptimo). Dicha relación se presenta en el **Cuadro Nº 10**.

Un primer análisis de dicha escala observaría que los niveles de exposición al riesgo Mayor y No Aceptable, pudiesen tener un rango muy extenso de valores; 4,0 a 7,99 y 8,0 a 25 puntos respectivamente, pero al realizar un análisis más riguroso, se debería observar que en realidad los niveles de exposición al riesgo con valores más altos, corresponden a las combinaciones entre los niveles de riesgo más severos y los niveles de eficiencia del control más Bajos, o a las

combinaciones entre los riesgos con severidad más altas y con controles que tienen un nivel de efectividad sólo de Regular.

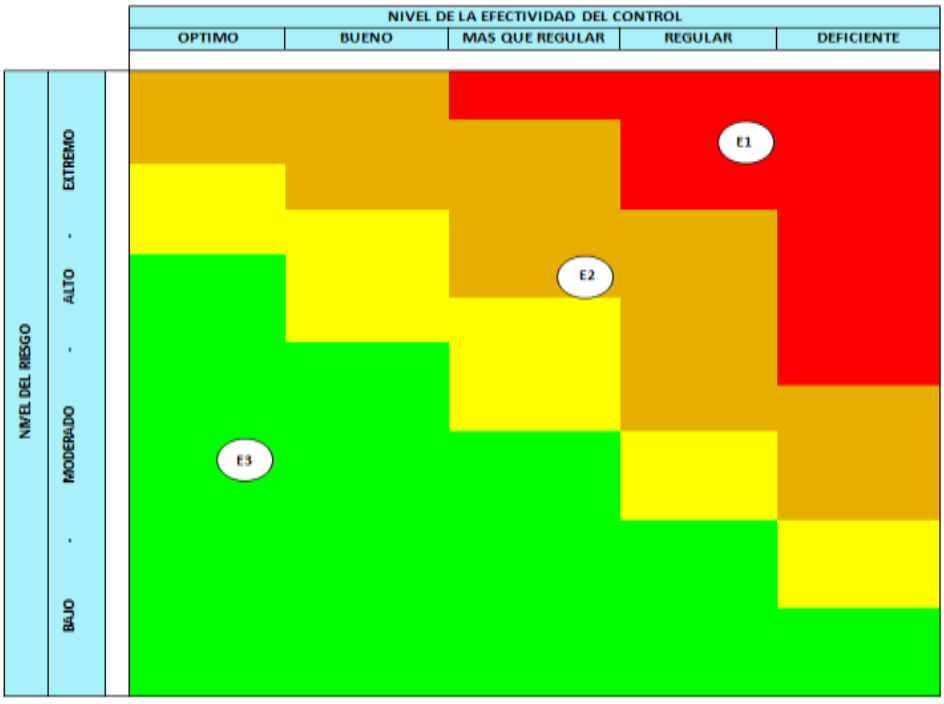
Por otra parte, los niveles de exposición al riesgo más bajos están conformados por las combinaciones entre los niveles de riesgos menos severas y los niveles de eficiencia del control más altos, o por las combinaciones entre riesgos con severidades Bajas y controles con niveles de efectividad Deficiente o Regular, o por las combinaciones entre riesgos con severidad altas, pero con controles con nivel de efectividad Óptimo o Bueno.

Por ejemplo, en el **Cuadro Nº 10** se observa que el nivel de exposición al riesgo E1 (Nivel de exposición al riesgo No Aceptable), está conformado por un nivel de severidad del riesgo, Extremo y un nivel de efectividad de control, Regular.

En el caso del nivel de exposición E2 (Nivel de exposición al riesgo Mayor), está conformado por un nivel de severidad del riesgo, Alto y un nivel de efectividad de control, Más que Regular.

Finalmente, el nivel de exposición E3 (Nivel de exposición al riesgo Menor), está conformado por un nivel de severidad del riesgo, Moderado y un nivel de efectividad de control, Óptimo.

Cuadro Nº 10: Relaciones Entre Severidad del Riesgo y Efectividad del Control que Determinan la Escala del Nivel de Exposición al Riesgo



ANEXO Nº 10

EJEMPLOS DE TÉCNICAS DE EVALUACIÓN DE RIESGOS Y OPORTUNIDADES

La metodología de evaluación de riesgos (identificación, análisis y valoración) de una entidad puede comprender una combinación de técnicas, junto con herramientas de apoyo. Por ejemplo, para la identificación de riesgos la dirección puede usar talleres interactivos de trabajo como parte de dicha metodología, con un monitor que emplee alguna herramienta tecnológica para ayudar a los participantes.

Entre los factores que influyen en la selección de las técnicas de evaluación del riesgo se cuentan los siguientes:

- La complejidad del problema y de los métodos que se necesitan para analizarlo.
- La naturaleza y el grado de incertidumbre de la evaluación del riesgo, basados en la cantidad de información disponible y que se requiere para satisfacer los objetivos.
- La amplitud de los recursos requeridos en función del tiempo y del nivel de conocimientos técnicos, de las necesidades de datos o de los costos.
- Si el método puede proporcionar un resultado cuantitativo.

Según la NCh-ISO 31010:2013 las técnicas de evaluación del riesgo (identificación, análisis y valoración) se pueden clasificar de varias maneras para ayudar a comprender sus cualidades relativas de solidez y debilidad. En la Norma, cada una de las 31 técnicas presentadas se desarrollan en detalle según la naturaleza de la evaluación que proporcionan, y se dan directrices para su aplicabilidad para determinadas situaciones. Algunos ejemplos de las técnicas clasificadas como “Muy Recomendadas” en la norma NCh-ISO 31010:2013 son las siguientes:

1.- Ejemplos de Técnicas de Identificación de Riesgos:

1.1.- Matriz de Consecuencias/Probabilidad

Es un medio de combinar clasificaciones cualitativas o semicuantitativas de consecuencia y probabilidad para producir un nivel de riesgo o una clasificación del riesgo. El formato de la matriz y las definiciones que se apliquen dependen del contexto en el que se usa, y es importante que se utilice un diseño apropiado a las circunstancias.

La matriz de consecuencia/probabilidad se utiliza para jerarquizar riesgos, orígenes de riesgo o tratamientos del riesgo sobre la base del nivel de riesgo. Normalmente, se utiliza como una herramienta de filtrado cuando se han identificado muchos riesgos, por ejemplo, para definir cuáles son los riesgos que necesitan análisis adicionales o más detallados, cuáles son los que se han de tratar primero, o cuáles se han de referenciar a un nivel de gestión más elevado.

1.2.- Tormenta de Ideas

Esta técnica implica el estímulo y el fomento de conversaciones fluidas entre un grupo de personas competentes, con objeto de identificar los posibles modos de falla y los peligros asociados, los riesgos, los criterios para la toma de decisiones, y/o las opciones de tratamiento. El término "tormenta de ideas" se utiliza frecuentemente de forma muy imprecisa cuando se aplica a cualquier tipo de debate en grupo. Sin embargo, la tormenta de ideas verdadera implica técnicas particulares para tratar de garantizar que se fuerza la imaginación de las personas mediante las ideas y declaraciones de otras personas del grupo.

En esta técnica es muy importante la facilitación eficaz e incluye la estimulación del debate desde el principio, las indicaciones periódicas del grupo sobre otras áreas importantes, y la aceptación de los resultados obtenidos en el debate (que normalmente suele ser bastante animado).

1.3.- Técnica Delphi

Un medio de combinar las opiniones de expertos que puede apoyar la identificación del origen y de la influencia, la estimación de la probabilidad y de la consecuencia, y la valoración del riesgo. Es una técnica de colaboración para crear el consenso entre expertos. Implica el análisis independiente y la votación de los expertos.

2.- Ejemplos de Técnicas de Análisis de Riesgos:

2.1.- Estructura “¿Y Sl…?” (SWIFT)

Es un sistema para ayudar a un equipo en la identificación de riesgos. Normalmente se utiliza dentro de un taller de trabajo dirigido. Por lo general está relacionado con una técnica de análisis y valoración del riesgo.

2.2.- Análisis de Modos y Efectos de Fallas (FMEA)

Es una técnica que identifica los modos y mecanismos de falla y sus efectos.

Existen varios tipos de análisis FMEA: FMEA del Diseño (o del producto), que se aplica a componentes y a productos; FMEA del Sistema, que se aplica a sistemas; FMEA del Proceso, que se aplica a procesos de fabricación y de montaje; FMEA de la organización gubernamental y FMEA del Software.

El FMEA puede ir seguido por un análisis de criticidad que defina la importancia de cada modo de falla de forma cualitativa, semicuantitativa o cuantitativa (FMECA2). El análisis de criticidad se puede basar en la probabilidad de que el modo de falla provocará la falla del sistema, o en el nivel de riesgo asociado al modo de falla, o en un número de prioridad del riesgo.

3.- Ejemplos de Técnicas de Valoración de Riesgos:

3.1.- Análisis de Peligros y de Puntos Críticos de Control (HACCP)

Es un sistema metódico, proactivo y preventivo para asegurar la calidad del producto, la fiabilidad y seguridad de los procesos, mediante la medición y monitoreo de las características específicas que se requiere que estén dentro de unos límites definidos.

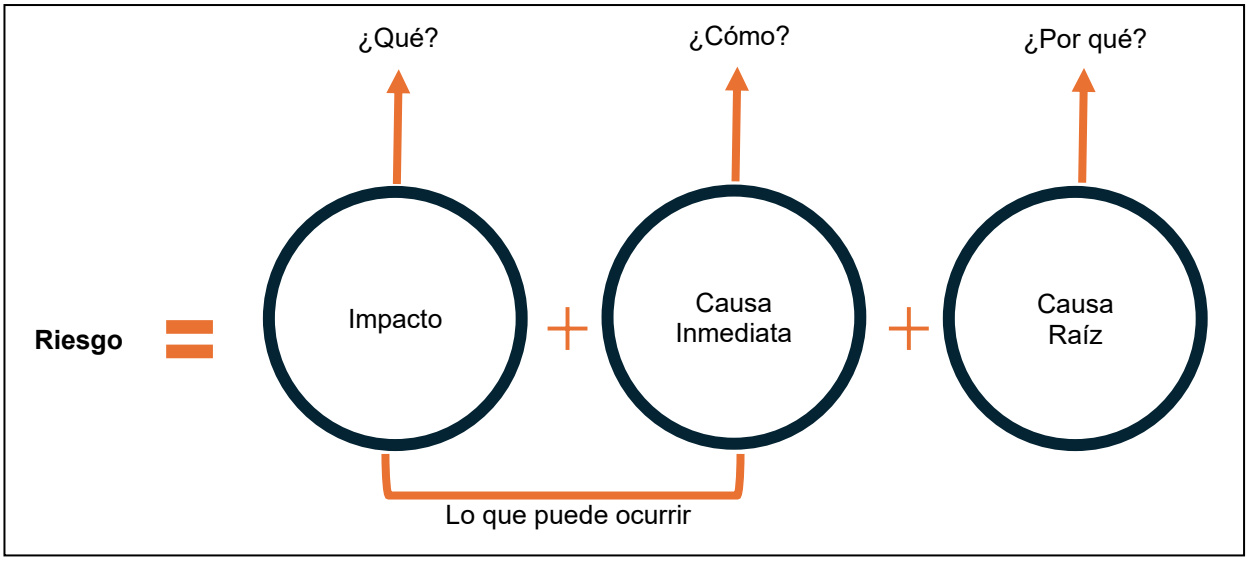
3.2.- Análisis de la Causa Raíz (RCA)

El análisis de una pérdida importante para prevenir que vuelva a ocurrir se conoce como Análisis de la Causa Raíz (RCA), Análisis de Falla de la Causa Raíz (RCFA) o análisis de pérdida. El análisis RCA se centra en las pérdidas de activos debido a diversos tipos de fallas, mientras que el análisis de pérdidas se aplica principalmente a las pérdidas financieras o económicas debidas a factores externos o a catástrofes. Este análisis intenta identificar las causas raíz u originales en vez de tratar únicamente los síntomas inmediatamente obvios. Se reconoce que la acción correctiva no siempre puede ser totalmente eficaz y que puede ser necesaria una mejora continua. El análisis RCA se aplica con bastante frecuencia para la evaluación de una pérdida importante, pero también se puede utilizar para analizar pérdidas sobre una base más global para determinar donde se pueden realizar mejoras.

ANEXO Nº 11

TÉCNICA PARA LA REDACCIÓN DE RIESGOS[19]

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el gestor del proceso como para personas ajenas al proceso. Para lo anterior, se sugiere una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE, analizando los siguientes elementos:



Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

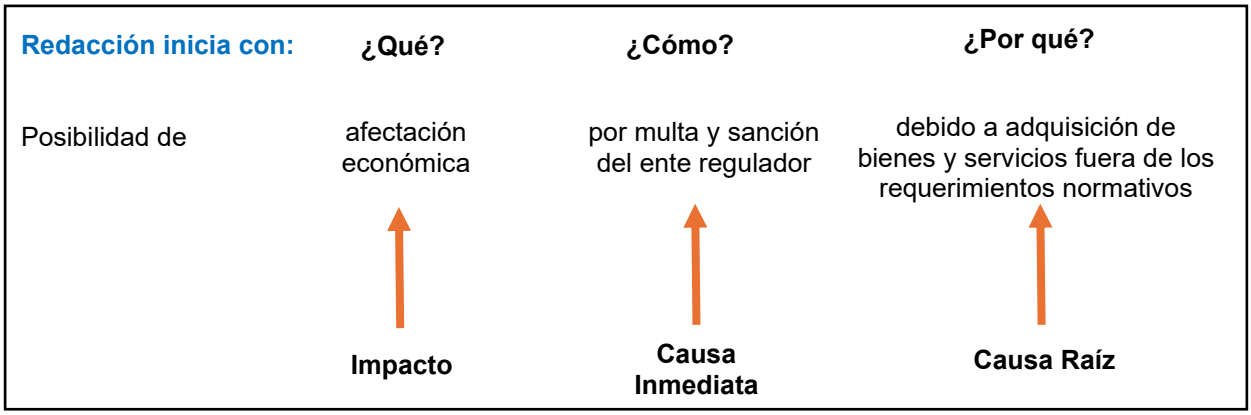
Causa raíz: es la causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

[19] Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Ejemplo:

Proceso: gestión de compras

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación



Descripción del riesgo Ejemplo:

Posibilidad de afectación económica por multa y sanción del ente regulador debido a adquisición de bienes y servicios fuera de los requerimientos normativos.

Premisas para una adecuada redacción del riesgo

1. No describir como riesgos omisiones ni desviaciones del control.

   Ejemplo: Riesgo de pérdida de datos debido a la omisión de copias de seguridad regulares.

   Correcto: Posibilidad de pérdida de datos debido a fallas en los sistemas de almacenamiento de información

2. No describir causas como riesgo.

   Ejemplo: Riesgo de fallo en el sistema debido a la sobrecarga del servidor.

   Correcto: Posibilidad de interrupción en el servicio debido a fallos en el sistema.

3. No describir riesgos como la negación de un control.

   Ejemplo: Riesgo de fraude por falta de auditorías internas.

   Correcto: Posibilidad de fraude en los procesos financieros.

4. No existen riesgos transversales, lo que pueden existir son causas transversales.

   Ejemplo: Riesgo transversal de fallos operativos en toda la organización.

Correcto: Posibilidad de fallos operativos en los sistemas de TI debido a la falta de capacitación adecuada del personal y a la deficiencia en la infraestructura tecnológica.

"En este ejemplo correcto, el riesgo se describe de manera específica (fallos operativos en los sistemas de TI) y se mencionan las causas transversales (falta de capacitación adecuada del personal y deficiencia en la infraestructura tecnológica) que pueden afectar múltiples áreas de la organización. Este enfoque permite identificar claramente el riesgo y sus causas sin generalizarlo como transversal."

ANEXO N° 12

CONCEPTOS SOBRE DELITOS DE LAVADO DE ACTIVOS (LA), FINANCIAMIENTO DEL TERRORISMO (FT) Y DELITOS FUNCIONARIOS (DF)

Este anexo ha sido formulado con el aporte de los especialistas de la Unidad de Análisis Financiero (UAF), con la finalidad de entregar conceptos y definiciones básicas sobre delitos de lavado de activos (LA), financiamiento del terrorismo (FT) y delitos funcionarios (DF).

Para mayor información sobre la materia, se recomienda acceder a la página web de la UAF (www.uaf.cl).

A.- LAVADO DE ACTIVOS (LA)

El que de cualquier forma oculte o disimule el origen ilícito de determinados bienes, a sabiendas de que provienen, directa o indirectamente, de la perpetración de hechos constitutivos de alguno de los delitos base, o bien, a sabiendas de dicho origen, oculte o disimule estos bienes.

El que adquiera, posea, tenga o use los referidos bienes, con ánimo de lucro, cuando al momento de recibirlos ha conocido su origen ilícito.

A.1.- Características del Lavado de Activos

Según la Unidad de Análisis Financiero (UAF), el fenómeno del lavado de activos presenta una serie de características que son las que sirven de explicación al proceso que pretende darle apariencia de legalidad a recursos que tienen un origen ilícito, entre las que destacan:

- **Naturaleza internacional**

El fenómeno del lavado de activos se vería en extremo limitado si no existiera un entorno internacional liberalizado. Esto es así, porque alejar el origen ilícito de los recursos implica un importante desplazamiento de los recursos del lugar donde se originaron, a fin de dificultar “su persecución por parte de las autoridades y facilitar su encubrimiento”.

Quienes se dedican a esta actividad se benefician de la diversidad de los sistemas jurídicos sobre la materia en los distintos países del mundo, las deficiencias de su normativa, las debilidades institucionales, etc., que les permiten eludir a las autoridades que persiguen estos delitos, aprovechándose de esas debilidades.

- **Volumen del fenómeno**

Es prácticamente imposible señalar los montos que genera a escala mundial la delincuencia organizada, y que son objeto del proceso de lavado de activos, ya que debido a su naturaleza ilícita no se cuenta con estadísticas.

No obstante, organismos y grupos de importancia universal, como la Organización de las Naciones Unidas (ONU), el Fondo Monetario Internacional (FMI), así como el Grupo de Acción Financiera (GAFI), en informes y artículos sobre el tema han puesto de manifiesto que se trata de sumas verdaderamente considerables.

La cifra más citada de los montos asociados al lavado de activos es la entregada por el FMI en el año 1988, la cual indica que se encontraría entre el 2% y 5% del PIB mundial. Un análisis de los resultados de diversos estudios sugiere que esta cifra asciende al 3,6% del PIB mundial, equivalente a cerca de US$2,1 billones de dólares (2009). Por eso, resulta evidente que el volumen de la actividad revela la magnitud del fenómeno, por lo que atenta contra el orden social, económico y político de los países, así como la estabilidad de los mercados financieros globales.

- **Profesionalización**

Dados los altos volúmenes envueltos en el proceso de lavado de activos, y la complejidad que conlleva la estructuración de operaciones para tener éxito en insertar en el sistema financiero con apariencia de legalidad activos que tienen un origen ilícito, se requiere que quienes estén al frente del diseño de las estrategias para tal propósito sean auténticos profesionales, de la banca, finanzas, contabilidad, leyes, que tengan por demás un amplio conocimiento del entorno regulatorio internacional sobre la materia, a fin de poder aprovechar las debilidades existentes en los distintos países.

- **Variedad y variación de las técnicas empleadas**

El éxito del lavado de activos requiere la utilización de una amplia gama de técnicas, a través de las cuales, en las distintas etapas del fenómeno, logren eludirse las regulaciones preventivas dispuestas por la autoridad.

Es por ello que el Grupo de Acción Financiera (GAFI) monitorea y realiza informes anuales respecto de las técnicas o tipologías usadas por los lavadores, para proporcionar a las autoridades del ámbito preventivo y persecutorio, las herramientas indispensables para el diseño de sus políticas. A su vez, proporciona las nuevas señales de alerta que hayan sido detectadas, de manera que sean utilizadas por las entidades reportantes para la detección de operaciones sospechosas. Esto, debido a que los lavadores van innovando su forma de operar para evitar ser descubiertos, por lo que las tipologías y señales de alerta también van cambiando.

B.- DELITOS BASE O PRECEDENTES

También conocidos como delitos precedentes o subyacentes. Son aquellos en que se originan los recursos ilícitos que los lavadores de dinero buscan blanquear. En la normativa chilena están descritos en la Ley N° 19.913, artículo 27, letras a y b. Entre otros, se incluye al narcotráfico, financiamiento del terrorismo, el tráfico de armas, la malversación de caudales públicos, el cohecho, el tráfico de influencias, el contrabando (artículo 168 de la Ordenanza General de Aduanas), el uso de información privilegiada, la trata de personas, la asociación ilícita, el fraude y las exacciones ilegales, el enriquecimiento ilícito, la producción de material pornográfico utilizando menores de 18 años, y el delito tributario (artículo 97, N°4, inciso 3° del Código Tributario), entre otros.

El listado completo de los delitos precedentes de lavado de activos se encuentra disponible en la página web de la UAF (www.uaf.cl). Es importante destacar que a las instituciones públicas no les corresponde detectar ningún tipo de delito. Su deber es reportar las operaciones sospechosas que adviertan en el ejercicio de sus funciones.

C.- FINANCIAMIENTO DEL TERRORISMO (FT)

La ley Nº 18.314 que determina conductas terroristas y fija su penalidad, en su artículo 8 incluye el delito de financiamiento del terrorismo "El que por cualquier medio, directa o indirectamente, solicite, recaude, o provea fondos con la finalidad de que se utilicen en la comisión de cualquiera de los delitos terroristas señalados en el artículo 2°, será castigado con la pena de presidio menor en su grado medio a presidio mayor en su grado mínimo, a menos que en virtud de la provisión de fondos le quepa responsabilidad en un delito determinado, caso en el cual se le sancionará por este último título, sin perjuicio de lo dispuesto en el artículo 294 bis del Código Penal."

D.- DELITOS FUNCIONARIOS (DF)

Los delitos funcionarios o delitos de corrupción son todas aquellas conductas ilícitas cometidas por funcionarios públicos en el ejercicio de sus cargos, o aquellas que afectan el patrimonio del Fisco en sentido amplio. Estos delitos, tipificados principalmente en el Código Penal, pueden ser cometidos activa o pasivamente por funcionarios públicos, definidos como todo aquel que desempeñe un cargo o función pública, sea en la Administración Central o en instituciones o empresas semifiscales, municipales, autónomas u organismos creados por el Estado o dependientes de él, aunque no sean del nombramiento del Jefe de la República ni reciban sueldos del Estado.

Entre los delitos precedentes de lavado de activos se contemplan algunos delitos funcionarios, por lo tanto, no todos los delitos funcionarios son delitos precedentes de lavado de activos.

Los delitos funcionarios precedentes de lavado de activos, según la ley N° 19.913, son:

- **Cohecho**: También conocido como soborno o "coima", es cometido por quien ofrece, y por quien solicita o acepta en su condición de funcionario público, dinero a cambio de realizar u omitir un acto que forma parte de sus funciones. Se considera que se comete el delito de cohecho incluso si no se realiza la conducta por la que se recibió dinero.

- **Cohecho a funcionario público extranjero**: Incurren en él quienes ofrecen, prometen o dan un beneficio económico, o de otra índole, a un funcionario público extranjero para el provecho de éste o de un tercero, con el propósito de que realice u omita un acto que permitirá obtener o mantener un negocio, o una ventaja indebida en una transacción internacional.

- **Fraudes y exacciones ilegales**: Incluyen el fraude al fisco; las negociaciones incompatibles con el ejercicio de funciones públicas; el tráfico de influencias cometido por la autoridad o funcionario público que utiliza su posición para conseguir beneficios económicos para sí o para terceros; y exacciones ilegales, consistentes en exigir en forma injusta el pago de prestaciones multas o deudas.

- **Malversación de caudales públicos**: Cuando se utilizan recursos fiscales, de cualquier clase, para un fin distinto al que fueron asignados.

- **Prevaricación**: Delito que comete un juez, una autoridad o un funcionario público, por la violación a los deberes que les competen cuando se produce una torcida administración del derecho.

E.- OPERACIÓN SOSPECHOSA

La Ley N° 19.913, en su artículo 3°, define como operación sospechosa "todo acto, operación o transacción que, de acuerdo con los usos y costumbres de la actividad de que se trate, resulte inusual o carente de justificación económica o jurídica aparente o pudiera constituir alguna de las conductas contempladas en el artículo 8º de la ley Nº 18.314 (de conductas terroristas), o sea realizada por una persona natural o jurídica que figure en los listados de alguna resolución del Consejo de Seguridad de las Naciones Unidas, sea que se realice en forma aislada o reiterada".

F.- REPORTE DE OPERACIÓN SOSPECHOSA (ROS)

El Reporte de Operación Sospechosa es la remisión de la información que ha tenido a la vista la institución y que ha considerado sospechosa mediante el sistema seguro UAF.

G.- FUNCIONARIO RESPONSABLE

Funcionario responsable de reportar operaciones sospechosas a la Unidad de Análisis Financiero, y de coordinar políticas y procedimientos para prevenir los delitos de lavado de activos, delitos funcionarios y financiamiento del terrorismo en los Servicios Públicos.

ANEXO N°13

EJEMPLOS DE SEÑALES DE ALERTA GENÉRICAS PARA DELITOS LA/FT/DF

Este anexo se ha formulado con el aporte de los especialistas de la Unidad de Análisis Financiero (UAF), con la finalidad de entregar conceptos y definiciones básicas sobre delitos de lavado de activos (LA), financiamiento del terrorismo (FT) y delitos funcionarios (DF).

Para más información sobre la materia, se recomienda acceder a la página web de la UAF (www.uaf.cl).

Las señales de alerta de delitos LA/FT/DF se pueden concebir como; indicadores, indicios, condiciones, comportamientos o síntomas de ciertas operaciones o personal que podrían permitir potencialmente detectar la presencia de una operación sospechosa de lavado de activos, delitos funcionarios o financiamiento del terrorismo[20].

Estas materias producto de los cambios de la ley 19.913, que se plasmaron en la ley 20.818, y del Oficio Circular N° 20/2015 del Ministerio de Hacienda, han relevado la necesidad de que sean conocidas por todo el personal de las organizaciones públicas incluidas en el alcance de estas disposiciones.

Es de vital importancia que las instituciones públicas, en base a la identificación y análisis de riesgos asociados al lavado de activos, delitos funcionarios o financiamiento del terrorismo, generen sus propias señales de alerta, que les permitirá fortalecer el sistema de Prevención de Delitos LA/FT/DF implementado en la organización.

También se recomienda que las organizaciones gubernamentales revisen periódicamente la Guía Señales de Alerta, publicada en la página web de la Unidad de Análisis Financiero (UAF): http://www.uaf.gob.cl/entidades/tipo_senales.aspx

A continuación, se mencionan solo a modo de ejemplo, señales de alerta genéricas, que se pueden identificar en las actividades operativas en cualquier tipo de organización y que pueden ser indicativas, debiendo examinarse debidamente para ver si corresponden a situaciones anómalas. Sin perjuicio de lo anterior, las señales de alerta siempre deben ser identificadas y analizadas de acuerdo con el contexto del sector donde está incorporada la organización.

[20] Definición adaptada de la (1) Guía de Recomendaciones para el Sector Público en la Implementación del Sistema Preventivo contra los Delitos funcionarios, Lavado de Activos y Financiamiento del Terrorismo y del (2) Catálogo de Delitos Precedentes de Lavado de Dinero en Chile, ambos emitidos por la Unidad de Análisis Financiero (UAF).

Estos ejemplos de señales de alerta genéricas fueron recopilados desde fuentes de información provenientes de; la Unidad de Análisis Financiero (UAF), del Grupo de Acción Financiera (GAFI), de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUCD), de la Dirección de Compras y Contratación Pública (ChileCompra), y del Consejo de Auditoría Interna General de Gobierno (CAIGG).

I.- ASOCIADAS A LA PROBIDAD FUNCIONARIA

- Recibir, en el cumplimiento de funciones públicas, donaciones, regalos o cualquier otro bien o servicio bajo cualquier concepto, proveniente de personas naturales o jurídicas.
- Uso de fondos públicos en actividades que no sean reconocidas como gastos de representación de la organización gubernamental.
- Uso de fondos públicos para actividades o compras ajenas a la organización gubernamental.
- Uso de fondos públicos para la compra de regalos o donaciones que no estén autorizadas por ley.
- Uso del automóvil institucional para motivos personales y/o fuera de días laborales sin justificación alguna.
- Adquisición de activos innecesarios para la organización gubernamental o que no cumplen con lo requerido por ésta, usualmente con el propósito de obtener una “comisión” del proveedor.

II.- ASOCIADAS A CONFLICTOS DE INTERÉS

- Relaciones cercanas de parentesco, sociales o de negocios de una de las contrapartes una operación con un funcionario público relacionado a la aceptación de dicha operación.
- Funcionarios públicos que ejercen como propietarios, directores o ejecutivos de una persona jurídica que participa directa o indirectamente de una licitación o contrato.
- Una Persona Expuesta Políticamente (PEP) es director o propietario efectivo de una persona jurídica, la cual, a su vez, es contratista de una organización gubernamental.

III.- ASOCIADAS A MANEJO DE INFORMACIÓN

- Otorgamiento de privilegios o permisos distintos al perfil del usuario de una cuenta, o a usuarios no autorizados.
- Funcionario público que divulga información personal de otros funcionarios de su organización gubernamental a empresas que manejan bases de datos.
- Funcionario público que revela información secreta de su organización gubernamental a los medios de comunicación o a las entidades reguladas por su institución, pudiendo recibir

algún tipo de retribución por ello.

- Funcionario que revela, de forma ilegal, información confidencial a determinada(s) empresa(s), en el marco de una licitación pública.

- Proveedor que no cumple con alguna cláusula de confidencialidad estipulada en un contrato de prestación de servicios.

- Existencia de evidencias que soportan el sabotaje en el uso de claves de acceso para el ingreso a los sistemas.

- Existencia de evidencias que soportan un posible ocultamiento de la información y/o maquillaje de la información reportada.

IV.- ASOCIADAS A PROCESO DE FISCALIZACIÓN Y SANCIÓN DE ENTIDADES REGULADAS

- Actualizar el registro con datos de entidades reguladas desajustados de la realidad o derechamente falsos, por incentivos o relaciones inadecuadas del funcionario con ellos.

- Favorecer a entidades reguladas en procedimientos infraccionales sancionatorios.

- Funcionarios que omiten ejercer las funciones de control y sanción asignadas a la institución pública.

V.- ASOCIADAS A FUNCIONARIOS DE LA ADMINISTRACIÓN PÚBLICA

- Funcionario público que se niega o dificulta la prestación de sus servicios, sugiriendo realizar pagos irregulares para agilizar su cometido o bien para pasar por alto un determinado trámite.

- Funcionarios públicos que, pese a no atender público, son visitados regularmente por clientes externos.

- Acciones demostradas de obstrucción de las investigaciones, tales como pérdida de expedientes de investigaciones disciplinarias, ruptura deliberada de las cadenas de custodia de la información, entorpecimiento de las visitas de las autoridades competentes de realizar el control, pérdida de computadores que contienen información relacionada, etcétera.

- Frecuentemente es renuente a entregar información rutinaria al auditor o fiscalizador.

- Funcionario público que, con frecuencia recibe y acepta obsequios y regalías por parte de determinadas empresas.

- Funcionarios o directivos de organizaciones gubernamentales que repentinamente presentan cambios en su nivel de vida o presentan comportamientos poco habituales.

- Funcionarios públicos que con frecuencia permanecen en la oficina más allá de la hora del

cierre o concurren a ella por fuera del horario habitual sin causa justificada.

- Funcionarios públicos que dificultan o impiden que otro personal atienda a determinados clientes /usuarios.
- Funcionarios públicos que frecuente e injustificadamente se ausentan del lugar del trabajo.
- Funcionarios públicos que, a menudo, se descuadran en la caja con explicación insuficiente o inadecuada.
- Funcionarios públicos renuentes a hacer el uso de su feriado legal (vacaciones).
- Gran centralización de varias funciones en una misma persona y resistencia a delegar trabajo.
- Utilización de equipos computacionales y técnicos para trabajar fuera del horario laboral, sin justificación.
- La información proporcionada por la persona no se condice con la información pública que se dispone (declaraciones de patrimonio o remuneraciones oficiales publicadas).

VI.- ASOCIADAS A INVENTARIOS

- Alta cantidad de ajustes de inventario por responsable y por proveedor.
- Alto nivel de mermas por tipo de inventario, locación, etcétera.
- Antigüedad excesiva de mercadería en tránsito.
- Falta de controles de ingreso y egreso de bienes para reparación.
- Identificar ítems con costo o cantidades negativas.
- Identificar un mismo ítem con diferente costo unitario según locación.
- Ítems con variaciones de costos mayores a un cierto porcentaje, entre períodos, definidos por la organización.
- Ítems con vida útil (antes de la fecha de vencimiento) inferior a un número de días, definidos por la organización.
- Ítems depositados en lugares de difícil acceso o sitios inusuales que hacen difícil su revisión o se encuentran inmovilizados durante mucho tiempo.
- Modificaciones a los stocks mínimos de seguridad.
- Movimientos de inventarios duplicados.

- Programas de inventarios donde varios usuarios pueden modificar los datos.
- Ítems en stock inmovilizados durante mucho tiempo.
- Altos niveles de devoluciones por ítem/proveedor.

VII.- ASOCIADAS A TRANSACCIONES FINANCIERAS UTILIZANDO FONDOS PÚBLICOS

- Cheques anulados y no reemitidos, cuando sí correspondía.
- Cheques emitidos no asociados a órdenes de pago o duplicados.
- Cobros de cheques en efectivo por terceros por sumas significativas de dinero provenientes desde cuentas de una institución pública.
- Créditos bancarios por depósito, no asociados a liquidaciones de Tesorería.
- Cuentas bancarias que no se concilian de manera oportuna.
- Débitos y créditos bancarios no asociados a cheques emitidos o generados por transferencias inconsistentes.
- Depósito frecuente de cheques girados desde cuentas de organizaciones gubernamentales que son depositados en cuentas de particulares y que inmediatamente son retirados o transferidos.
- Depósitos frecuentes de cheques girados por la organización gubernamental desde la cuenta de un particular.
- Operaciones fraccionadas para eludir sistemas de control.
- Pagos a la orden de una empresa o persona distinta del proveedor.
- Retiros de dinero con cargo a cuentas públicas que se realizan en lugares y horas diferentes o con patrones de comportamiento que no están acordes a este tipo de cuentas.
- Arreglos especiales con bancos para establecer transacciones poco claras (giros, préstamos, etcétera.)
- Ausencia, alteración o simulación de documentos que soportan el origen de las transacciones financieras relacionadas con la organización gubernamental.
- Solicitudes de pago de último momento, sin el suficiente respaldo documental.
- Colocar en la caja chica vales o cheques sin fecha, con fecha adelantada o con fecha atrasada.

- Deudas vencidas impagas por mucho tiempo.
- Documentos financieros frecuentemente anulados.
- Facturas en fotocopias sin certificación de autenticidad (cuando corresponda).
- Falta de control de consistencia en rendiciones de fondos de caja.
- Inexistencia de revisión independiente de las conciliaciones bancarias y movimientos de dinero en la organización gubernamental.
- Ruptura de correlatividad en la numeración de los cheques.

VIII.- ASOCIADAS AL PAGO DE REMUNERACIONES

- Contratación o ingresos de funcionario público que fue desafectado o despedido, sin justificación.
- Cuando se dificulta la distinción entre los flujos de fondos personales y aquellos derivados de su actividad profesional.
- Depósitos de sueldos en cuentas bancarias a nombre de un beneficiario distinto del personal.
- Funcionarios con datos compartidos (nombre, domicilio, RUT) y con distinto número de carpeta o registro.
- Ingresos y egresos de funcionario público, sin autorización adecuada.
- Pagos a funcionarios fantasmas (empleados inventados), sueldos ficticios o duplicados.
- Pagos realizados a funcionarios públicos por conceptos distintos a los estipulados para sus remuneraciones.
- Ranking de horas extras por empleado/jefe autorizante, falsificación de carga horaria.

IX.- ASOCIADAS A PROCESOS DE CONTRATACIÓN DE FUNCIONARIOS PÚBLICOS

- Contratar a funcionarios incumpliendo el procedimiento de reclutamiento interno o legal.
- Contratar a personal en cargos de la organización gubernamental en razón de la obtención de contraprestaciones de provecho particular para el funcionario involucrado.
- Contratar en cargos de la organización gubernamental a personas con relaciones de parentesco consanguíneo o por afinidad, en cualquiera de sus grados, respecto del funcionario de la organización gubernamental a cargo de dicha contratación.
- Cambios frecuentes de perfiles de cargos y del manual de funciones para ajustar los requerimientos a los perfiles específicos de las personas que se quiere beneficiar.

- Contratación de personas que no cumplen con los perfiles requeridos para los cargos en cuestión o con las condiciones e idoneidad requerida para el cargo, especialmente en los cargos de supervisión, o que demuestren posteriormente una evidente incompetencia en el ejercicio de sus funciones.

- Creación de cargos y contratación injustificada de nuevos funcionarios que no corresponden a las necesidades reales de la organización gubernamental, en algunas oportunidades en calidad de asesores que solventen las deficiencias que se presentan en el perfil del directivo contratado.

- Interés de una de las contrapartes por acordar servicios sin contrato escrito.

- Modificaciones frecuentes e injustificadas de las tablas de honorarios, o desconocimiento de las mismas a la hora de determinar los honorarios de las personas que se vincularán.

X.- ASOCIADAS A LICITACIONES Y COMPRAS PÚBLICAS

1.- Planificación de Compras

- Juntar pedidos y hacer pedidos excesivos y en corto plazo de entrega para beneficiar al proveedor que tiene un acuerdo especial.

- Modificaciones significativas del plan anual de adquisiciones de la entidad en un período relativamente corto.

- Fragmentación de licitaciones y/o contratos por motivos injustificados y repetitivos.

2.- Proceso de Licitación y Adjudicación

- Otorgar contratos a proveedores en razón de la existencia de lazos de parentesco consanguíneo o por afinidad en cualquiera de sus grados.

- Detección de errores idénticos o escrituras similares en los documentos presentados por distintas empresas en una licitación.

- Evidencia de actuaciones de abuso de poder de los jefes, es decir, de la utilización de las jerarquías y de la autoridad para desviar u omitir los procedimientos al interior de la institución pública, para de esta forma adaptar el proceso de acuerdo con los intereses particulares (Ejemplo: Excesivo interés de los directivos, imposición de funcionarios para que participen indebidamente en el proceso, etcétera).

- Falta de división de responsabilidad de funcionarios que participan en el diseño de las pautas de licitaciones y aquellos que evalúan las propuestas.

- Imposibilidad para identificar la experiencia de los proponentes a una licitación.

- Presentación de varias propuestas idénticas en el proceso de licitación o de adquisición.

- Proveedor hace declaraciones falsas o inconsistentes con el propósito de adjudicarse una determinada licitación o contrato.

- Proveedor presenta vínculos con países o industrias que cuentan con historial de corrupción.

- Sociedades que participan de un proceso de licitación y/o contrato con el sector público que presentan el mismo domicilio, mismos socios o mismos directivos.

- Sospechas del involucramiento de terceros en la elaboración de los estudios previos a una licitación y/o compra pública, o que estos estuvieron notablemente direccionados.

- Proveedor carece de experiencia con el producto, servicio, sector o industria, cuenta con personal insuficiente o mal calificado, no dispone de instalaciones adecuadas, o de alguna otra forma parece ser incapaz de cumplir con la operación propuesta.

- Adjudicación del contrato a un proponente que no cumple con los requisitos solicitados en las bases de licitación publicadas.

- Presencia de múltiples y pequeñas sociedades recién constituidas en un proceso de licitación, las que no presentan la capacidad financiera para adjudicarse la misma y que a la vez se asocian a un mismo proponente.

- Tiempo entre cierre y adjudicación muy acotado. Esto puede ser indicativo de 1) la evaluación no se hizo adecuadamente o 2) existía un proveedor seleccionado con anterioridad, a quien le será adjudicado el proceso.

- Un mismo proveedor gana todas las licitaciones o ciertas empresas presentan frecuentemente ofertas que nunca ganan, o da la sensación de que los licitantes se turnan para ganar licitaciones.

- Destinación de grandes recursos de capital a obras de primera necesidad como alcantarillado, suministro de agua potable, expansión de la red eléctrica, etcétera, que son iniciadas, pero nunca terminadas, o que superan varias veces el costo presupuestal.

- Usos de trato directo sin causa legal que lo justifique y/o sin resolución que lo autorice.

- Realización del proceso de compra sin haber cumplido de manera adecuada con el procedimiento interno y/o el reglamento de compras públicas (evaluación técnica y económica del bien o servicio, constitución de un comité evaluador, aprobación de los estudios técnicos, entre otros).

- Elaboración de conceptos técnicos equivocados, mal intencionados o direccionados por parte de los funcionarios que intervienen en el proceso de licitación, con el objeto de favorecer a un posible oferente del mercado.

- Licitante seleccionado no cumple con requisitos solicitados por la institución pública contratante.

- Determinación de una única persona para la conformación y evaluación de las propuestas que se presentan a la institución pública, sin que intervengan otros funcionarios de la institución pública.

- Evidencias de que el personal involucrado en el proceso de licitación y/o compras carecen del perfil o de las competencias, habilidades, experiencia y conocimiento adecuado sobre los procedimientos necesarios para el desarrollo del proceso.

- Presentación de propuestas y/o adjudicación de contratos por valores significativamente mayores o inferiores a los precios de mercado de los bienes o servicios en cuestión.

- Marcado interés de algún funcionario evaluador por una propuesta en particular, cuando existen otras propuestas en igualdad de condiciones.

- Sospechas relacionadas con solicitudes de “sobornos” o “coimas” realizadas para avalar estudios o emitir opiniones técnicas favorables a un proponente, por parte de la persona relacionada al proceso de licitación pública y/o contratación.

- Una de las contrapartes de una licitación u contrato involucra a múltiples intermediarios o a terceros que no se requieren en la operación.

3.- Procesos de Pagos de Contratos

- Crecimiento excesivo e injustificado de las cuentas por cobrar de la institución pública, con respecto al comportamiento de los mismos rubros en periodos anteriores.

- Definición desproporcionada de los anticipos asignados sin que se garantice la respectiva ejecución del contrato.

- Diferencias entre orden de compra, informes de recepción y factura por proveedor, entre esta última y la orden de pago.

- Dispersión de recursos a terceros diferentes a los gestores del contrato, como consecuencia de esquemas de subcontratación y/o tercerización de las obligaciones contractuales.

- Existencia de evidencias que soportan que se ha realizado alteración de facturas y adulteración de documentos.

- Facturas de varios proveedores en un mismo papel, formato y hasta con el mismo detalle.

- Inexistencia de soportes que prueben la recepción de los dineros como consecuencia de la recaudación dentro de los términos establecidos en el contrato.

- Pagos fechados antes del vencimiento de la factura.

- Proporción excesiva que representan las notas de débito y de crédito sobre las compras de cada proveedor.

- Proveedores con pagos individualmente inmateriales, pero significativos en su conjunto.

4.- Procesos de Gestión de Contratos

- Liquidación anticipada de contratos de manera frecuente en la institución pública, sin la justificación necesaria.

- Omisión reiterada de los procedimientos administrativos para hacer efectiva las condiciones acordadas en caso de incumplimiento de contrato.

- Pérdida de documentos esenciales, en especial las pólizas de seguro y otras garantías a través de las cuales se busca proteger los intereses de la institución pública.

- Pérdida de expedientes de investigaciones disciplinarias e imposición de obstáculos a los procesos de reubicación laboral por parte de los funcionarios involucrados en la conformación y supervisión de los contratos.

- Ambigüedad y generalidad en los términos de referencia de la contratación, modificaciones injustificadas, prórrogas de los mismos y/o cambios en la modalidad de contratación, que impiden la pluralidad de oferentes.

- Diferencia marcada en la interpretación técnica de aspectos relevantes para la ejecución del contrato.

- Modificaciones sustanciales e injustificadas en las condiciones y/o requisitos contractuales establecidos inicialmente para el cumplimiento del contrato (Ejemplo: Ampliación de términos, prórrogas y adiciones injustificadas en el contrato).

- Realización de pagos por adelantado o de aumentos en las compensaciones antes de terminar un proyecto u otorgarse una concesión, contrato u otro tipo de acuerdo, incluso por trabajos o asesorías no realizadas.

- Alta rotación o cambios injustificados de los funcionarios responsables de hacer la conformación y/o supervisión de los contratos.

- Resistencia de los funcionarios a suministrar la información relacionada con los contratos.

- Visitas frecuentes de un directivo de una entidad contraparte de un contrato con la institución pública, sin que haya razones institucionales para que estas se realicen.

- Ruptura de la correlatividad en la numeración de las órdenes de compra, informes de recepción y órdenes de pago.

Para conocer más sobre riesgos relacionados con el Proceso de Compras Públicas, se recomienda leer el Documento Técnico N° 122: “Evaluación de Actividades Asociadas a la Probidad Administrativa en las Compras Públicas en el Estado”, emitido por el Consejo de Auditoría Interna General de Gobierno (CAIGG).

ANEXO N° 14

SEÑALES DE ALERTA LA/FT/DF NO ASOCIADAS CON LOS RIESGOS INCLUIDOS EN LA MATRIZ DE RIESGOS ESTRATÉGICA

Sin perjuicio de las señales de alerta de delitos LA/FT/DF incluidas en la Matriz de Riesgos Estratégica, adicionalmente se deberá:

- Identificar riesgos o señales de alerta LA/FT/DF en los procesos, subprocesos, etapas, proyectos, sistemas, etc. que no hayan sido considerados en la Matriz de Riesgos Estratégica, por no estar dentro del porcentaje mínimo (valor porcentual mínimo) de procesos críticos que deben analizarse en la organización, según lo informado por el CAIGG. En el caso que todos los procesos de la Organización estén incluidos en la Matriz de Riesgos Estratégica, no será necesario considerar este requerimiento.

- Identificar cuando sea posible, otras señales de alerta de delitos LA/FT/DF relacionados con procesos, subprocesos, etapas, etc. que por su naturaleza y características, no se han podido asociar a los riesgos operativos incluidos en la Matriz de Riesgos Estratégica. Se recomienda ver ejemplos en **Anexo N° 13**.

Para levantar la información sobre estas materias debe considerarse la siguiente estructura:

Cuadro Nº 1: Estructura de Información a Levantar Relacionada con Señales de Alerta LA/FT/DF No Asociadas con los Riesgos Incluidos en la Matriz de Riesgos Estratégica

Proceso, Subproceso, Etapa, Sistema, Proyecto, etc. (1)	Identificación/ Descripción de la Señal de Alerta LA/FT/DF (2)	Cargo(s) Funcionario Relacionado(s) (3)	Control Asociado (4)	Nivel de Cobertura de la Señal de Alerta (5)	Medidas Correctivas y/o Preventivas (6)

(1) Identificar el ámbito organizacional donde se encuentra ubicada la Señal de Alerta LA/FT/DF. Por ejemplo; proceso, subproceso, etapa, sistema, proyecto, etc.
(2) Describir la Señal de Alerta LA/FT/DF de la manera más completa posible.
(3) Se debe identificar el o los cargos funcionarios que se relacionan de manera teórica y más directamente con el riesgo y/o Señal de Alerta LA/FT/DF.
(4) Describir el control mitigante existente, que está asociado a la Señal de Alerta LA/FT/DF.
(5) Identificar el nivel de cobertura del control sobre la señal de alerta. Las categorías de los niveles de cobertura son: “Alta”, “Media”, “Baja”, según la descripción contenida en el Cuadro N° 2.
(6) Cuando corresponda, se deben describir medidas correctivas y/o preventivas que la administración tomará; idealmente para mejorar los niveles de cobertura del control asociado a la Señal de Alerta LA/FT/DF, clasificados como “Baja” y “Media”.

Cuadro Nº 2: Escala del Nivel de Cobertura de la Señal de Alerta LA/FT/DF

NIVEL DE COBERTURA	DESCRIPCIÓN
BAJA	El control asociado a la señal de alerta de delitos LA/FT/DF es insuficiente, por lo que la cobertura es baja, dejando a la organización muy expuesta a la materialización del delito (riesgo)
MEDIA	El control asociado a la señal de alerta de delitos LA/FT/DF es regular, por lo que la cobertura es media, dejando a la organización regularmente expuesta a la materialización del delito (riesgo)
ALTA	El control asociado a la señal de alerta de delitos LA/FT/DF es adecuado, por lo que la cobertura es alta, dejando a la organización poco expuesta a la materialización del delito (riesgo)

Como ya se señaló, el Consejo de Auditoría Interna General de Gobierno podrá definir qué informes derivados del Proceso de Gestión de Riesgos desarrollado por las Organizaciones Gubernamentales deben ser reportados, así como la oportunidad y formato de dichos reportes.

ANEXO Nº 15

ASPECTOS CLAVES DEL CONTROL (GGSAI Nº 3)

Control

El glosario de las NOGAI define control como:

"Cualquier medida que tome la Dirección, el Consejo y otras partes para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos."

Los controles son los mecanismos fundamentales mediante los cuales una entidad responde a los riesgos que enfrenta. Para el auditor interno, el análisis de controles no debe limitarse a su existencia en papel, sino que debe considerar:

• **Diseño:** ¿Está bien formulado el control para mitigar el riesgo? ¿Es lógico, oportuno, específico y coherente con el proceso?
• **Implementación y funcionamiento:** ¿Está el control en operación? ¿Se aplica de forma constante y de acuerdo con el diseño? ¿Se documenta su ejecución?

Los controles operativos relacionados con la mitigación del riesgo más conocidos incluyen:

Preventivos: Evitan que ocurra el riesgo (ej. límites de aprobación, validación de datos, firma dual).
Detectivos: Identifican la ocurrencia del riesgo tras su manifestación (ej. conciliaciones, alertas, análisis de excepciones).
Correctivos: Restauran condiciones normales o eliminan impactos (ej. recuperación de pagos, medidas disciplinarias).

También se clasifican como automáticos (integrados en sistemas), manuales (realizados por personas), o híbridos (combinación). La auditoría interna debe validar no solo su existencia, sino su efectividad en la operación para mitigar los riesgos.

Tipología de controles relevantes para la planificación del trabajo

Al momento de planificar un trabajo, no basta con identificar si existen controles: también hay que entender qué tipo de controles son, cómo funcionan y en qué contexto operan. Algunos controles tienen un rol más estratégico, otros son operativos o de respaldo, y su revisión ayuda a enfocar mejor el trabajo y aplicar un enfoque basado en riesgos de forma más eficaz.

1. Control clave

Una actividad diseñada para reducir el riesgo asociado a un objetivo crítico del negocio. En el sector público se puede utilizar un lenguaje más acorde con la misión y la gestión institucional para referirse al término "negocio", por ejemplo: objetivo crítico institucional / Objetivo misional.

Ejemplo: Verificación automatizada de requisitos y antecedentes del beneficiario antes de aprobar el subsidio → Asegura que solo personas o entidades elegibles accedan a recursos públicos.

2. Control secundario

Una actividad diseñada para reducir riesgos asociados a objetivos del negocio que no son críticos para la supervivencia o el éxito de la organización, o bien, para funcionar como respaldo de un control clave.

Ejemplo: Revisión aleatoria de rendiciones de bajo monto una vez al año → No sustituye el control obligatorio en rendiciones de alto riesgo, pero agrega una capa adicional de revisión.

3. Controles de nivel superior

Estos controles los ejerce la Alta Dirección o instancias de gobernanza, y cumplen una función más estratégica que operativa. Están pensados para supervisar transversalmente el funcionamiento general de la organización y detectar desvíos importantes antes de que se conviertan en problemas.

Algunos ejemplos son:

- Reuniones ejecutivas donde se revisan periódicamente los resultados clave.
- Informes consolidados de monitoreo de procesos críticos.
- Evaluaciones realizadas por comités de auditoría o de riesgos.

Ejemplo: El comité de riesgos institucional revisa mensualmente un tablero con indicadores clave (KPI) de todos los departamentos. Si detecta desviaciones en presupuestos, cumplimiento normativo o incidentes operativos, exige explicaciones y propuesta de corrección formales. Este tipo de control permite anticipar problemas antes de que escalen, fortalece la cultura organizacional de control y mejora la capacidad de respuesta.

4. Controles compensatorios

Son mecanismos que no eliminan el riesgo directamente, pero ayudan a reducirlo cuando un control clave está ausente, es débil o no se puede aplicar. Pueden ser soluciones temporales o permanentes, siempre que mantengan el riesgo en niveles aceptables.

Para que un control compensatorio sea válido, la función de auditoría interna debe verificar que:

Reduce la exposición al riesgo de forma aceptable, según el umbral definido por la entidad.
Cumple, al menos en parte, la función del control principal que falta.
Está bien documentado y se revisa periódicamente para asegurarse de que funciona.

Desde el punto de vista de auditoría interna, si se detecta que falta un control clave, se deben identificar y probar los controles compensatorios disponibles. Según sus resultados, se ajusta la valoración del riesgo residual.

Ejemplo: En una entidad pequeña, donde no es posible separar las funciones de autorización y registro de pagos por falta de personal, el jefe del área que no participa en la preparación de pagos revisa semanalmente los desembolsos, analiza la documentación de respaldo y firma un acta como evidencia. Aunque este control no elimina el riesgo de fraude, lo reduce al incorporar una revisión independiente.

5. Controles con diseño adecuado

Son controles bien estructurados, con funciones claras y responsables definidos. Tienen una frecuencia de aplicación establecida y tienen evidencia sistemática de que realmente se están ejecutando. Además, están directamente relacionados con los riesgos que buscan controlar y responden a una lógica operativa coherente.

Ejemplo: En el proceso de rendición de viáticos y pasajes, puede haber un procedimiento formal que exija presentar los comprobantes originales, la firma del jefe directo y una revisión por parte de finanzas dentro de un plazo de cinco días. Si además el sistema registra todo electrónicamente y emite alertas cuando se incumplen los plazos, se trata de un control con buen diseño; ya que está documentado, tiene responsables asignados, parte del proceso está automatizado y existe supervisión efectiva.

Controles como este son más fáciles de evaluar. Al estar bien definidos, permiten hacer pruebas precisas y emitir una opinión técnica sólida. Por eso, son importantes de incluir en el programa de trabajo cuando se busca validar si el sistema de control interno es realmente efectivo.

6. Controles afectados por cambios recientes

Este tipo de controles pueden haber perdido efectividad por modificaciones en su entorno interno o externo. Los motivos más comunes son:

- Cambios en los sistemas de información.
- Reestructuraciones organizacionales.
- Cambios en normativas o en procedimientos internos.

Ejemplo: Si se implementa un nuevo sistema de gestión documental y no se replican correctamente los permisos de acceso desde el sistema anterior, puede pasar que ciertos usuarios tengan acceso a información sin los mismos controles que antes. Esto genera una exposición que antes no existía y que puede no estar bien cubierta.

En estos casos, es necesario revisar el control en detalle. Los cambios pueden haber creado brechas o debilitado el control sin que nadie lo haya notado. Por eso, requieren atención especial para evitar exposiciones imprevistas y asegurar que el sistema de control sigue siendo efectivo frente a las nuevas condiciones.

7. Controles a nivel de entidad

Estos pueden dividirse en dos categorías:

- Controles de gobernanza y

- Controles de supervisión de la gestión.

Los controles de gobernanza son establecidos por el Jefe de Servicio y la Alta Dirección con el fin de instaurar la cultura de control de la organización y proporcionar orientación que respalde los objetivos estratégicos.

Los controles de supervisión de la gestión son establecidos por la Dirección en las unidades de negocio y niveles operativos de la organización, con el objetivo de reducir riesgos en dichas unidades y aumentar la probabilidad de que se logren sus objetivos.

8. Controles en distintos niveles organizacionales

• Control a Nivel de Entidad (Entity-Level Control)

Un control que opera en toda la entidad y, por tanto, no está limitado ni asociado a procesos individuales.

Ejemplo: El establecimiento de un Código de Ética Institucional aprobado por el Jefe de Servicio, obligatorio para todos los funcionarios públicos de la entidad.

• Control a Nivel de Proceso (Process-Level Control)

Una actividad que opera dentro de un proceso específico, con el propósito de alcanzar objetivos propios de ese proceso.

Ejemplo: Un procedimiento formal para la revisión y aprobación de solicitudes de subsidios sociales, incluyendo pasos definidos, roles, plazos y documentación requerida.

• Control a Nivel de Transacción (Transaction-Level Control)

Una actividad que reduce el riesgo asociado a un conjunto o variedad de tareas operativas o transacciones específicas dentro de una organización.

Ejemplo: La verificación automática de la identidad del beneficiario antes de emitir el pago de un subsidio mediante cruce de datos con el registro civil.

9. Clasificación simultánea de controles

Un mismo control puede pertenecer simultáneamente a varias categorías dependiendo de su naturaleza y función. Por ejemplo, un control puede ser a la vez:

- Un control a nivel de entidad,
- Un control clave (por su impacto en la mitigación de un riesgo crítico), y
- Un control de tipo detectivo (su función es Identificar la ocurrencia del riesgo tras su manifestación).

Sin embargo, otras combinaciones no son compatibles. Por ejemplo, un control no puede ser al mismo tiempo clave, de nivel de entidad y secundario o de transacción, ya que estas últimas categorías responden a niveles de relevancia y alcance distintos.

Aunque estas clasificaciones pueden resultar complejas, con la práctica y el análisis de controles en los procesos se adquiere una mejor comprensión de cómo interactúan y se superponen estas categorías.

ANEXO Nº 16

CRITERIOS PARA LA APLICACIÓN, REGISTRO Y EVALUACIÓN DE CONTROLES EN LA MATRIZ DE RIESGOS

1. Definición de Control Interno

El control interno es un proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento[21].

Esta definición refleja ciertos conceptos fundamentales. El control interno:

- Está orientado a la consecución de objetivos en una o más categorías–operaciones, información y cumplimiento.
- Es un proceso que consta de tareas y actividades continuas–es un medio para llegar a un fin, y no un fin en sí mismo.
- Es efectuado por las personas–no se trata solamente de manuales, políticas, sistemas y formularios, sino de personas y las acciones que éstas aplican en cada nivel de la organización para llevar a cabo el control interno.
- Es capaz de proporcionar una seguridad razonable–no una seguridad absoluta, al consejo y a la alta dirección de la entidad.
- Es adaptable a la estructura de la entidad–flexible para su aplicación al conjunto de la entidad o a una filial, división, unidad operativa o proceso de negocio en particular.

Esta definición es intencionadamente amplia. Incluye conceptos importantes que son fundamentales para las organizaciones respecto a cómo diseñar, implantar y desarrollar el control interno, constituyendo así una base para su aplicación en entidades que operen en diferentes estructuras organizacionales, sectores y regiones geográficas.

Respecto de los Procesos de Control se pueden decir que corresponden a las políticas, procedimientos (manuales y automáticas) y actividades, los cuales forman parte de un enfoque de control, diseñados y operados para asegurar que los riesgos estén contenidos dentro del las tolerancias establecidas por el proceso de evaluación de riesgos nivel que una organización está dispuesta a aceptar[22].

Por su parte, el Control se puede considerar como cualquier medida que tome la dirección, el Consejo y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas[23].

[21] COSO I
[22] COSO I
[23] Normas Generales de Auditoría Interna y de Gestión del Colegio de Contadores de Chile y Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna – THEIIA.

Se pueden complementar estas definiciones señalando que el control ha sido definido bajo dos grandes puntos de vista, un punto de vista limitado y un punto de vista amplio.

Desde el punto de vista limitado, puede señalarse que, el control se concibe como la verificación a posteriori de los resultados conseguidos en el seguimiento de los objetivos planteados y el control de gastos invertido en el proceso realizado por los niveles directivos.

Desde un punto de vista amplio, puede señalarse que el control es una actividad no sólo a nivel directivo, sino de todos los niveles y miembros de la entidad, orientando a la organización hacia el cumplimiento de los objetivos propuestos bajo mecanismos de medición cualitativos y cuantitativos. Este enfoque hace énfasis en los factores sociales y culturales presentes en el contexto institucional ya que parte del principio que es el propio comportamiento individual quien define en última instancia la eficacia de los métodos de control elegidos por la gestión

El control es una etapa primordial en la administración, pues, aunque una entidad tenga excelentes controles teóricos, una estructura organizacional adecuada y una dirección eficiente, es necesario que exista un mecanismo que verifique e informe si los hechos y actividades de la entidad se están desarrollando según los objetivos.

2. Tipos de Actividades de Control

Entre los tipos de actividades de control de transacciones más comunes se encuentran:

- **Autorizaciones y Aprobaciones:** Una autorización confirma que una transacción es válida según los criterios definidos por la organización. Una autorización se expresa mediante una conformidad formal proporcionada por una persona con un perfil adecuado y previamente definido en la organización.

  Ejemplo: autorización de un informe de rendición de gastos una vez que ha revisado su razonabilidad y que su monto y naturaleza es consistente con la política de la organización en esta materia.

- **Verificaciones:** Las verificaciones comparan dos o más elementos entre sí o bien comparan un elemento con criterios definidos en una política o norma, y llevan a cabo un seguimiento cuando los dos elementos en cuestión no coinciden o el elemento no es coherente con los criterios de la política o norma.

  Ejemplo: comparaciones automatizadas en el sistema para determinar, entre otras cosas; que esté aprobado el pago por el usuario que tenga el perfil adecuado, que existan comprobantes que justifiquen el desembolso, que se haya pagado el importe correcto y que esté bien registrado el pago.

- **Controles Físicos:** Los equipos, existencias, valores, efectivo y otros bienes o activos se resguardan de manera física, se contabilizan periódicamente y se comparan con los montos reflejados en los registros y documento de control.

  Ejemplo: bodegas de bienes con acceso restringido y protegidas con guardias o con vigilancia a través de cámaras digitales.

- **Controles sobre Datos Vigentes:** Los datos vigentes, como puede ser por ejemplo el archivo maestro de perfiles de autorización en una organización, se utilizan a menudo para contrastar automáticamente la autorización de determinadas transacciones contra quienes tienen formalmente esa responsabilidad dentro de un proceso de negocio.
  Ejemplo: contraste y verificación de autorizaciones válidas para la orden de compra, el envío y la factura; autorización de la aplicación de descuentos pactados según la política de ventas de la organización.

- **Reconciliaciones:** Las reconciliaciones comparan dos o más elementos de datos y, en caso de que se identifiquen diferencias, se deben tomar medidas por las personas responsables para definir los datos correctos.

  Ejemplo: Realizar conciliación diaria sobre el efectivo recibido, con respecto a los saldos contables, con la finalidad de evaluar su integridad, precisión y validez.

- **Controles de Supervisión:** Los controles de supervisión corresponden a las actividades de revisión periódicas o permanentes que se realizan sobre las actividades de control de transacciones habituales y que se asocian a las de mayor riesgo para la organización.

  Ejemplo: Supervisión periódica de que las modificaciones de los programas fuentes informáticos estén autorizadas por las personas responsables según la política de la organización.

3. Requisitos del Control Adecuado

Un control adecuado es el que está presente si la dirección ha planificado y organizado (diseñado) las operaciones de manera tal que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica[24].

En consideración a lo anterior, un control, para poder ser declarado como adecuado debe tener propiedades como las siguientes:

- **Permitir la corrección de fallas y errores:** El control debe detectar e indicar errores de planeación, organización o dirección.
- **Contribuir a la previsión de fallas o errores futuros:** el control, al detectar e indicar errores actuales, debe prevenir errores futuros, ya sean de planeación, organización o dirección.

4. Importancia del Control

El control es importante toda vez que permite medir el desempeño organizacional y cómo se van cumpliendo los objetivos de una entidad. Hasta el mejor de los planes se puede desviar. El control se emplea entre otros propósitos para:

- **Mejorar la calidad de los procesos y actividades**: Las fallas se detectan y el proceso se corrige para eliminar errores.
- **Enfrentar el cambio**: Este forma parte ineludible del ambiente de cualquier organización. Las directrices de gobierno cambian, el comportamiento de los usuarios de los servicios o

[24] Normas Internacionales para el Ejercicio de la Profesión de Auditoría Interna - IIA

beneficios se modifica, surgen exigencias nuevas, aparecen tecnologías emergentes, se aprueban o modifican leyes y reglamentos, etc. La función del control sirve a la dirección para responder a las amenazas o las oportunidades de todo ello, porque les ayuda a detectar los cambios que están afectando los productos y los servicios de sus organizaciones.

- **Agregar valor**: Los tiempos veloces de los ciclos son una manera de obtener ventajas competitivas. El principal objetivo de una organización debería ser "agregar valor" a su producto o servicio, de tal manera que los usuarios puedan aprovechar eficiente y eficazmente sus beneficios. Con frecuencia, este valor agregado adopta la forma de una calidad por encima de la medida lograda aplicando procedimientos de control.
- **Facilitar la delegación y el trabajo en equipo**: La tendencia contemporánea hacia la administración participativa también aumenta la necesidad de delegar autoridad y de fomentar que los empleados trabajen juntos en equipo. Esto no disminuye la responsabilidad última de la dirección. Por el contrario, cambia la índole del proceso de control. Por tanto, el proceso de control permite que la dirección controle el avance de los funcionarios, sin entorpecer su creatividad o participación en el trabajo.

5. Secuencia Típica de Control Adecuado

- **Fijación de estándares**: Es la primera etapa del control, que establece los estándares o criterios de evaluación o comparación. Un estándar es una norma o un criterio que sirve de base para la evaluación o comparación de alguna cosa.
- **Selección de puntos críticos de control**: Debe definirse cuáles serán los puntos o aspectos claves de control que deben monitorearse.
- **Comparación y verificación contra los estándares.** Se compara el desempeño con lo que fue establecido como estándar, para verificar si hay desvío o variación, esto es, algún error o falla con relación al desempeño esperado.
- **Reporte de desviaciones significativas al nivel jerárquico correspondiente.** En el caso de existir desviaciones del estándar, debe informarse al jefe correspondiente
- **Tomar acciones correctivas.** La acción correctiva es siempre una medida de corrección y adecuación de algún desvío o variación con relación al estándar esperado.
- **Determinación si la acción tomada es efectiva para corregir las desviaciones tomadas.**
- **Revisar y modificar los estándares si corresponde.**

6. Elementos Básicos Considerados en el Modelo para Determinar un Control Adecuado

Son los medios, mecanismos o procedimientos que permiten alcanzar los objetivos de control. Comprenden las políticas específicas, los procedimientos, los planes de la organización (incluida la división de las tareas) y los dispositivos físicos (tales como cerraduras o alarmas contra incendio), si bien no se limitan exclusivamente a estos aspectos. Los controles deben proporcionar una seguridad razonable de que se logren continuamente los objetivos del control interno. Para ello, deben ser eficaces y estar diseñados de forma que operen como un sistema integrado y no individualmente.

Los controles, para que sean adecuados, deben cumplir con el propósito previsto en la aplicación real. Es posible que los controles diseñados para funcionar en un ambiente manual no sean eficaces en uno automatizado. Por consiguiente, los controles seleccionados deben cumplir el propósito previsto y funcionar siempre que el caso lo requiera. En cuanto a su eficiencia, los

controles deben estar diseñados para poder obtener el máximo beneficio con un esfuerzo adecuado. Los controles que se examinen para verificar su adecuación deben ser los que se utilizan en la práctica y deben ser evaluados periódicamente para asegurar su aplicación constante en la prevención de riesgos.

Los elementos que se presentan a continuación son los que se utilizan generalmente en una estructura de control interno adecuada. Los métodos y procedimientos específicos que se describen en relación con cada uno de ellos no pretenden ser exhaustivos sino que deben ser considerados como ejemplos. Entre otros se cuentan: la organización, la documentación, el registro oportuno y adecuado de las transacciones y hechos, autorización y ejecución de las transacciones y hechos, división de las tareas, supervisión y acceso a los recursos y registros y responsabilidad ante los mismos.

a) Documentación en Papel y/o Medios Electrónicos

Deben documentarse las estructuras de control interno y todas las transacciones y hechos internos, incluyendo sus objetivos y procedimientos de control, y todos los aspectos pertinentes de las transacciones y hechos significativos. Asimismo, la documentación en papel y electrónica debe estar disponible y ser fácilmente accesible para su verificación por el personal apropiado y los auditores.

La documentación relativa a las estructuras de control interno debe incluir aspectos sobre la estructura y políticas de una institución, sobre sus categorías operativas, objetivos y procedimientos de control. Esta información debe figurar en documentos tales como planes o guías, las políticas administrativas y los manuales de operación y de contabilidad.

La documentación sobre transacciones y hechos significativos debe ser completa y exacta y facilitar el seguimiento de la transacción o hecho, antes, durante y después de su realización.

La documentación de las estructuras de control interno, de las transacciones y de hechos importantes debe tener un propósito claro, ser apropiada para alcanzar los objetivos de la institución y servir a los directivos para controlar sus operaciones y a los auditores para analizar dichas operaciones.

En los casos en que existen sistemas informáticos integrados en la institución, que generen como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas, integridad, completitud, archivo o registro, accesibilidad y disponibilidad y no-repudio de la información.

b) Registro Oportuno y Adecuado de las Transacciones y Hechos

Las transacciones y hechos importantes deben registrarse inmediata y debidamente clasificados.

Las transacciones deben registrarse en el mismo momento en que ocurren a fin de que la información siga siendo relevante y útil para los directivos que controlan las operaciones y adoptan las decisiones pertinentes. Ello es válido para todo el proceso o ciclo de vida de una transacción; abarcando el inicio y la autorización, todos los aspectos de la transacción mientras se realiza y su anotación final en los registros. También conviene actualizar rápidamente toda la documentación con objeto de mantener su validez.

Se requiere, asimismo, una clasificación pertinente de las transacciones y hechos a fin de garantizar que la dirección disponga continuamente de una información fiable. Una clasificación pertinente significa organizar y procesar la información a partir de la cual se elaboran los informes, los planes y los estados financieros y presupuestarios.

El registro inmediato y pertinente de la información es un factor esencial para asegurar la oportunidad y fiabilidad de toda la información que la institución maneja en sus operaciones y en la adopción de decisiones.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto de la firma, integridad, completitud y archivo o registro.

c) Autorización y Ejecución de las Transacciones y Hechos

Las transacciones y hechos relevantes solo podrán ser autorizados en papel o electrónicamente y ejecutados por aquellas personas que actúen dentro del ámbito de sus competencias.

La dirección es quien decide el canje, la transferencia, la utilización o la asignación de fondos para atender metas específicas en condiciones particulares. La autorización es la principal forma de asegurar que sólo se efectúen transacciones y hechos válidos de conformidad con lo previsto por la dirección. La autorización debe estar documentada física o electrónicamente y ser comunicada explícitamente a los directivos y a los empleados, incluyendo los términos y condiciones específicos conforme a los cuales se concede una autorización. La conformidad con los términos de una autorización significa que los empleados ejecutan las tareas que les han sido asignadas de acuerdo con las directrices y dentro del ámbito de competencias establecido por la dirección o la legislación.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas e integridad de la información.

d) Segregación de Funciones

Las tareas y responsabilidades principales ligadas a la autorización, tratamiento, registro y revisión de las transacciones y hechos deben ser asignadas a personas diferentes.

Con el fin de reducir el riesgo de errores, despilfarros o actos ilícitos, o la probabilidad de que no se detecten este tipo de problemas, es preciso evitar que todos los aspectos fundamentales de una transacción u operación se concentren en manos de una sola persona o sección. Las funciones y responsabilidades deben asignarse sistemáticamente a varias personas para asegurar un equilibrio eficaz entre los poderes. Entre las funciones claves figuran la autorización y el registro de las transacciones, la emisión y el recibo de los haberes, los pagos y la revisión o fiscalización de las transacciones. Sin embargo, la colusión puede reducir o eliminar la eficacia de esta técnica de control interno.

Una pequeña organización puede que no tenga suficientes empleados para aplicar esta técnica plenamente. En tal caso, la dirección debe ser consciente del riesgo que ello implica y compensar

el defecto con otros controles. La rotación del personal contribuye a que los aspectos centrales de las transacciones o hechos contables no se concentren en una sola persona por un espacio de tiempo prolongado. Debe promoverse e incluso exigirse también el uso del período vacacional anual para ayudar a reducir estos riesgos.

e) Supervisión

Debe existir una supervisión para garantizar el logro de los objetivos de control interno.

Los supervisores deben examinar y aprobar cuando proceda, el trabajo encomendado a sus subordinados. Asimismo, deben proporcionar al personal las directrices y la capacitación necesarias para minimizar los errores, el despilfarro y los actos ilícitos y asegurar la comprensión y cumplimiento de las directrices específicas de la dirección.

La asignación, revisión y aprobación del trabajo del personal exige:

- Indicar claramente las funciones y responsabilidades del trabajo del empleado.
- Examinar sistemáticamente el trabajo de cada empleado, en la medida que sea necesario.
- Aprobar el trabajo en puntos críticos del desarrollo para asegurarse de que avanza según lo previsto.

La asignación, revisión y aprobación del trabajo del personal debe tener como resultado el control apropiado de sus actividades. Ello incluye: la observancia de los procedimientos y requisitos aprobados, la constatación y eliminación de los errores, los malentendidos y las prácticas inadecuadas, la reducción de las probabilidades de que ocurran o se repitan actos ilícitos y el examen de la eficiencia y eficacia de las operaciones. La delegación del trabajo de los supervisores no exime a estos de la obligación de rendir cuentas de sus responsabilidades y tareas.

f) Acceso a los Recursos y Registros y Responsabilidades Ante los Mismos

El acceso a los recursos y registros debe limitarse a las personas autorizadas para ello, quienes están obligadas a rendir cuentas de la custodia o utilización de los mismos. Para garantizar dicha responsabilidad, se debe cotejar periódicamente los recursos con los registros y verificar si coinciden. La frecuencia de estas comparaciones depende de la vulnerabilidad y relevancia de los activos.

La restricción del acceso físico y lógico a los recursos permite reducir el riesgo de una utilización no autorizada o de pérdida y contribuir al cumplimiento de las directrices de la dirección. El grado de limitación depende de la vulnerabilidad de los recursos y del riesgo potencial de pérdida. Ambos deben evaluarse periódicamente. Por ejemplo, el acceso a los documentos sumamente vulnerables y la responsabilidad ante los mismos, tales como cheques en blanco, puede restringirse:

- Manteniéndolos en una caja fuerte.
- Asignando a cada documento un número de serie.
- Encargando su custodia a personas responsables.

- Al determinarse la vulnerabilidad de un activo, debe considerarse también su costo, la facilidad de transporte y el riesgo de pérdida o de utilización indebida.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas, integridad y accesibilidad y disponibilidad. Además de deberá evaluar los niveles de seguridad de los accesos lógicos a las bases de datos de la organización.

7.- Componentes y Principios del Marco Integrado de Control Interno – COSO I, versión 2013

El control interno es un proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento[25].

El Marco COSO versión 1992 fue mejorado en el 2013[26] a través de la ampliación de la categoría de objetivos de la información financiera, incluyendo otras formas importantes de reporting, como por ejemplo la información no financiera y el reporting interno. Asimismo, el Marco COSO I, versión 2013 refleja los cambios en el entorno empresarial y operativo de las últimas décadas, entre los que se incluyen:

- Las expectativas de supervisión del gobierno corporativo.
- La globalización de los mercados y las operaciones.
- Los cambios y el aumento de la complejidad de las actividades empresariales.
- Demandas y complejidades de las leyes, reglas, regulaciones y normas.
- Expectativas de las competencias y responsabilidades.
- Uso y dependencia de tecnologías en evolución.
- Expectativas relacionadas con la prevención y detección del fraude.

El Marco COSO I establece tres categorías de objetivos, que permiten a las organizaciones centrarse en diferentes aspectos del control interno:

- Objetivos operativos. Hacen referencia a la efectividad y eficiencia de las operaciones de la entidad, incluidos sus objetivos de rendimiento financiero y operacional, y la protección de sus activos frente a posibles pérdidas.
- Objetivos de información. Hacen referencia a la información financiera y no financiera interna y externa y pueden abarcar aspectos de confiabilidad, oportunidad, transparencia, u otros conceptos establecidos por los reguladores, organismos reconocidos o políticas de la propia entidad.
- Objetivos de cumplimiento. Hacen referencia al cumplimiento de las leyes y regulaciones a las que está sujeta la entidad.

[25] COSO I
[26] La Versión 2013 del Marco COSO sustituirá a la Versión 1992 al final del período de transición, es decir, el 15 de diciembre de 2014.

El control interno consta de cinco componentes integrados: Entorno de Control, Evaluación de Riesgos, Actividades de Control, Información y Comunicación y Actividades de Supervisión.
Existe una relación directa entre los objetivos, que es lo que una entidad se esfuerza por alcanzar, los componentes, que representa lo que se necesita para lograr los objetivos y la estructura organizacional de la entidad (las unidades operativas, entidades jurídicas y demás). La relación puede ser representada en forma de cubo.

- Las tres categorías de objetivos –operativos, de información y de cumplimiento– están representadas por las columnas.
- Los cinco componentes están representados por las filas
- La estructura organizacional de la entidad está representada por la tercera dimensión.

Además de este Marco, la organización COSO publicó simultáneamente el documento Control Interno sobre la Información Financiera Externa: un compendio de métodos y ejemplos para proporcionar enfoques prácticos y ejemplos que ilustran cómo los componentes y principios enunciados en el Marco se pueden aplicar en la preparación de los estados financieros.

Otra de las publicaciones emitidas por la organización COSO es la Gestión de riesgos Corporativos - Marco Integrado (Marco ERM). Este y el Marco COSO I son complementarios y no se sustituyen entre sí. Sin embargo, aunque estos marcos son diferentes y proporcionan enfoques distintos, abordan determinadas áreas comunes. El Marco ERM abarca también el control interno, y reproduce varias partes del texto del Control Interno - Marco Integrado original (COSO I).

En consecuencia, el Marco ERM sigue siendo un marco viable y adecuado para el diseño, la implementación, la ejecución y la evaluación de la gestión de riesgos corporativos.

El Marco COSO I, versión 2013, establece un total de diecisiete principios que representan los conceptos fundamentales asociados a cada uno de los cinco componentes integrados. Dado que estos diecisiete principios proceden directamente de los Componentes, una entidad puede alcanzar un control interno efectivo aplicando todos los principios. La totalidad de los principios son aplicables a los objetivos operativos, de información y de cumplimiento. A continuación se enumeran los principios que soportan los componentes del control interno.

Componentes y Principios del Control Interno

Entorno de Control

- La organización demuestra compromiso con la integridad y los valores éticos.
- La máxima autoridad[27] demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.
- La dirección establece, con la supervisión del consejo, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.
- La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en alineación con los objetivos de la organización
- La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.

[27] En las organizaciones del Sector Público el equivalente al Consejo es la Máxima Autoridad o Jefe de Servicio.

Evaluación de Riesgos

- La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.
- La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determinar cómo se deben gestionar.
- La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.
- La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.

Actividades de Control

- La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.
- La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.
- La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos que llevan dichas políticas a la práctica.

Información y Comunicación

- La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.
- La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.
- La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.

Actividades de Supervisión

- La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento.
- La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda.

Para mayor información se recomienda leer el Marco Integrado de Control Interno – COSO I, versión 2013, emitido por la organización COSO (www.coso.org).

8.-Identificación y Análisis de Controles Claves

Identificados los riesgos, es necesario identificar y analizar los controles claves existentes en la institución, los que teóricamente mitigan los riesgos, esto es, todas las medidas que ha tomado la administración con la finalidad de evitar la ocurrencia de un riesgo potencial. Estos controles

deben ser evaluados en el nivel de cumplimiento de los elementos de un control adecuado y calificados de acuerdo con su diseño, es decir, su oportunidad (en qué momento del proceso se aplican; preventivos, correctivos, detectivos), periodicidad (si son permanentes, periódicos u ocasionales), grado de automatización (manual, semi automatizado, 100% automatizado) y evaluados en términos del cumplimiento de normas específicas de control.
Los controles deben ser identificados con una descripción del mismo que contenga al menos los siguientes antecedentes:

- Qué se realiza.
- Cómo se realiza el control.
- Quién lo realiza.
- Cuándo lo ejecuta.

Por ejemplo, para describir un control de acceso a los servidores de la organización gubernamental, se sugiere:

- Restricciones de Acceso (**Qué**).
- Existe una restricción de acceso a la sala de servidores, ya que sólo pueden ingresar quienes cuentan con tarjeta especial y clave de acceso, la cual sólo se entrega a tres funcionarios responsables de la División de Sistemas (**Cómo**).
- La emisión de tarjeta de autorización para el acceso y la entrega de claves se realizan por el Jefe de la División de Sistemas, previa aprobación del Jefe de Servicio de los funcionarios habilitados (**Quién**).
- Las autorizaciones se revisan mensualmente por el Jefe de la División de Sistemas, que emite un reporte al Jefe de Servicio (**Cuándo**).

Control redactado de forma integrada

El acceso a la sala de servidores se encuentra restringido exclusivamente a tres funcionarios de la División de Sistemas, quienes cuentan con tarjeta especial y clave de acceso. La emisión de las tarjetas y la asignación de claves es realizada por el Jefe de la División de Sistemas, previa aprobación del Jefe de Servicio, y las autorizaciones vigentes son revisadas mensualmente, generándose un reporte formal al Jefe de Servicio.

Una vez determinada claramente la existencia de todos los controles asociados a los riesgos relevantes que operan en el proceso en estudio, será necesario en primer lugar, definir si existe uno o más controles asociados a cada riesgo específico identificado.

Cuando exista más de un control por riesgo específico, será necesario identificar si se trata de controles cuya presencia es clave o fundamental para mitigar la ocurrencia del riesgo, o si alguno de los controles identificados no tiene esa característica y sólo se trata de controles que no contribuyen significativamente a mitigar el riesgo. En general para este último tipo de controles, es recomendable informar a la Dirección, para su eliminación o fortalecimiento, si corresponde (relación costo/beneficio).

Cuando se identifique que un riesgo específico tiene varios controles asociados y éstos tienen distinto nivel de efectividad medida en forma individual, el auditor debe sólo evaluar el nivel de efectividad que se genera al actuar en conjunto los distintos controles clasificados como claves,

desechando para efectos de este análisis a los controles no fundamentales (ver ejemplo en páginas siguientes).

El segundo paso corresponde a determinar (identificar, analizar y cuantificar) el nivel de efectividad de los controles en base al diseño del control y cumplimiento de los elementos de un control adecuado. Nivel definido por los atributos periodicidad, oportunidad y nivel de automatización del control, en base al esquema que se presenta en la página siguiente.
El siguiente paso corresponde a analizar para cada uno de los controles claves identificados con los riesgos, el grado de cumplimiento de los elementos de un control adecuado.

En resumen, lo que se persigue con este procedimiento, no es sólo verificar la existencia y el grado de cumplimiento de normas específicas para todos los controles, sino que evaluar si existen controles claves o fundamentales asociados a un riesgo en particular y si estos además de cumplir con los elementos de un control adecuado, están diseñados con la finalidad de mitigar los efectos que se puedan producir ante la materialización del riesgo.

A continuación, se presenta un procedimiento que permite dejar evidencia del análisis realizado al auditor. Para este efecto, se sugiere utilizar el siguiente esquema:

Cuadro N° 1: Análisis de Controles Claves

Etapa	Riesgo Relevante	Descripción del Control identificado en el proceso (asociado a un riesgo determinado)	Importancia del control presente para mitigar los riesgos al interior del proceso	
			Clave/Fundamental	No es Fundamental

Ejemplo de determinación de una evaluación de la efectividad de los controles claves:

i.- Cuadro N° 2: Ejemplo para Identificación de Controles Claves en la Etapa "Cálculo de Horas Extraordinarias"

Etapa	Riesgo Relevante	Descripción del Control identificado en el proceso (asociado a un riesgo determinado)	Importancia del control presente para mitigar los riesgos al interior del proceso	
			Clave/ fundamental	No es fundamental
Cálculo de horas extraordinarias	Errores o irregularidades en el cálculo de las horas extraordinarias	Registro automatizado (**Qué**) en el sistema de control biométrico que registra las horas trabajadas y calcula aquellas que exceden de las 44 horas ordinarias (**Cómo**), donde diariamente se registran las horas y calcula semanalmente (**Cuándo**), por el responsable del sistema biométrico (**Quién**).	**X**	
		La visación (**Qué**)se efectúa mediante la revisión y aprobación del cálculo de horas para su pago (**Cómo**), mensualmente (**Cuándo**), por el Jefe de la Unidad de remuneraciones (**Quién**)	**X**	
		El encargado de remuneraciones lleva un archivador con el detalle de las horas extras por funcionario		**X**

En este caso, se identifican tres controles mitigantes asociados directa o indirectamente al riesgo "Errores o irregularidades en el cálculo de las horas extraordinarias", por lo que debe realizarse en primer lugar un análisis de la importancia de cada control para mitigar el riesgo, es decir, determinar si se trata de un control clave.

El resultado del análisis muestra en el ejemplo que, el control descrito como "El encargado de remuneraciones lleva un archivador con el detalle de las horas extras por funcionario", no es un control clave, por lo que no se analizará en cuanto al nivel de cumplimiento con los requisitos o normas que considera el modelo.

ii.- Cuadro N° 3: Ejemplo de Análisis del Cumplimiento de Requisitos del Modelo de Control en los Controles Mitigantes Examinados

Riesgo Relevante	Nivel de cumplimento de los elementos de control adecuado asociado Niveles de cumplimiento: adecuado, regular, insuficiente					
	Documentación	Registro	Autorización	División o Segregación	Supervisión	Acceso
Errores o irregularidades en el cálculo de las horas extraordinarias	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel regular
Conclusión respecto del nivel del control: **Adecuado**						

iii.- Cuadro N° 4: Ejemplo Determinación de la Efectividad de los Controles Claves

Controles Claves/fundamentales	Nivel de Cumplimiento de los elementos de control adecuado	Características en el diseño de los controles claves/fundamentales				
		Oportunidad	Periodicidad	Automatización	Clasificación	Valor
El sistema biométrico de control horario contiene un algoritmo que calcula las horas trabajadas, indicando en forma precisa aquellas que exceden de las 44 semanales. El jefe de remuneraciones revisa el reporte del sistema y aprueba el cálculo para su pago.	Adecuado respecto a los elementos de control del modelo	Preventivo (previene errores y se encuentra al principio del proceso)	Periódico (a la fecha de corte mensual para pago)	Automatizado y Manual	Óptimo	5

9.- Limitaciones de un Sistema de Control Interno

Si bien el control interno proporciona una seguridad razonable acerca de la consecución de los objetivos de la entidad, existen limitaciones. El control interno no puede evitar que se aplique un deficiente criterio profesional o se adopten malas decisiones, o que se produzcan acontecimientos externos que puedan hacer que una organización no alcance sus objetivos operacionales. Es decir, incluso en un sistema de control interno efectivo puede haber fallos. Las limitaciones pueden ser el resultado de:

- La falta de adecuación de los objetivos establecidos como condición previa para el control interno.
- El criterio profesional de las personas en la toma de decisiones puede ser erróneo y estar sujeto a sesgos.
- Fallos humanos, como puede ser la comisión de un simple error.
- La capacidad de la dirección de anular el control interno.
- La capacidad de la dirección y demás miembros del personal y/o de terceros, para eludir los controles mediante connivencia entre ellos.
- Acontecimientos externos que escapan al control de la organización.
- La relación costo beneficio: El control no debería superar el valor de lo que se quiere controlar.

Estas limitaciones impiden que la dirección de la entidad gubernamental tenga la seguridad absoluta de la consecución de los objetivos de la entidad, es decir, el control interno proporciona una seguridad razonable, pero no absoluta. A pesar de estas limitaciones inherentes, la dirección debe ser consciente de ellas cuando seleccione, desarrolle y despliegue los controles que minimicen, en la medida de lo posible, estas limitaciones.

10.- Descripción de Controles Claves

Al describir los controles existentes, se debe señalar al menos: la norma o guía que lo instruye, quién lo realiza, qué actividades desarrolla, cómo las ejecuta y cuándo y cómo se evidencia su cumplimiento (registros documentales o electrónicos en el sistema). Además, como ya se señaló, al describir los controles siempre se deben responder las preguntas, ¿qué?, ¿cómo?, ¿quién? y ¿cuándo?, esto es, debería especificarse qué se hace, cómo o de qué forma se lleva a efecto el control, quién lo ejecuta y cuándo.

Por tanto, en la descripción de los controles deberá utilizarse una redacción integrada, precisa y verificable, evitando la fragmentación explícita de sus componentes (¿qué se hace?, ¿cómo se ejecuta?, ¿quién es responsable? y ¿cuándo se realiza?).

El control deberá formularse como una acción completa y coherente, que permita comprender en una sola declaración su naturaleza, mecanismo de ejecución, responsable y periodicidad.

ANEXO Nº 17

EJEMPLO DE FORMATO DE PLAN DE COMUNICACIÓN Y CONSULTA

La comunicación y consulta puede y debe ser a través de un plan estructurado. Este plan de comunicación y consulta es fundamental para garantizar que todos los procesos de la matriz de riesgos sean gestionados de manera efectiva y que todas las partes interesadas estén informadas y comprometidas.

Plan de Comunicación y Consulta.

Elementos deseables que debe contener:

1. Objetivo del Plan

Establecer un sistema claro y efectivo de comunicación y consulta para identificar, evaluar y gestionar los riesgos asociados con el [proceso x]

Asegurar que todas las partes interesadas estén informadas, comprometidas y puedan contribuir a la gestión de riesgos.

2. Identificación de las Partes Interesadas

Internas:
Equipos de proyecto.
Departamentos de Finanzas, Ingeniería, y Legal.
Alta dirección del Ministerio.

Externas:
Comunidad local.
Contratistas y proveedores.
Autoridades locales y reguladoras.
Servicios de emergencia.
Medios de comunicación.

3. Estrategias de Comunicación

Reuniones:
Semanales con el equipo de proyecto.
Mensuales con contratistas y proveedores.
Trimestrales con la comunidad local y autoridades reguladoras.

Informes:
Informes quincenales internos sobre el progreso del proyecto y los riesgos.
Boletines mensuales para la comunidad local y partes interesadas externas.

Plataformas digitales:
Plataforma de gestión de proyectos para actualizaciones en tiempo real.
Correo electrónico y sitios web para distribuir información y recibir comentarios.

4. Métodos de Consulta

Encuestas y Cuestionarios:
Encuestas trimestrales a la comunidad local sobre el impacto del proyecto.

Talleres y Seminarios:
Talleres bimestrales con contratistas y proveedores para revisar riesgos y estrategias de mitigación.

Grupos Focales:
Grupos de trabajo con representantes de la comunidad y otras partes interesadas para discutir preocupaciones y sugerencias.

5. Procedimientos y Cronograma

Lanzamiento del Plan:
Fecha de inicio: [Fecha]
Presentación del plan a todas las partes interesadas.

Implementación Continua:
Reuniones semanales, mensuales y trimestrales según lo planificado.
Distribución de informes y boletines según el cronograma establecido.

Evaluaciones y Revisiones:
Evaluaciones semestrales del proceso de comunicación y consulta.
Adaptaciones y mejoras según los comentarios y retroalimentación recibidos.

6. Roles y Responsabilidades

Coordinador del Proyecto:
Responsable de la implementación general del plan.

Equipo de Comunicación:
Preparación y distribución de informes y boletines.
Organización de reuniones y talleres.

Responsables de Consulta:
Realización de encuestas y recolección de feedback.
Facilitación de grupos focales y talleres.

7. Medición y Seguimiento

Indicadores de Desempeño:
Número de reuniones realizadas y asistencia.
Cantidad y calidad de la retroalimentación recibida.
Número de encuestas completadas y resultados.

Herramientas de Seguimiento:
Registro de comunicaciones y consultas.
Plataforma digital para monitoreo de actualizaciones y seguimiento de riesgos.

8. Revisión y Mejora Continua

Evaluaciones periódicas:
Evaluaciones semestrales para revisar la efectividad del plan.

Retroalimentación y Mejora:
Solicitar retroalimentación continua de todas las partes interesadas.
Implementar mejoras basadas en la retroalimentación y las evaluaciones.

ANEXO Nº 18

EJEMPLO: INFORMACIÓN PARA EL TRATAMIENTO DE RIESGOS

Proceso transversal (1)	Proceso (2)	Ranking de procesos (3)	Subproceso (4)	Etapa (5)	Riesgo Específico (6)	Fuente del riesgo (7)	Tipo de riesgo (8)	Estrategia genérica (9)	Descripción de la estrategia a aplicar (10)	Efecto potencial en la severidad de riesgo y/o efectividad del control (11)	Responsable de la estrategia (12)	Plazo (13)	Indicador de logro (14)	Periodo Medición del Indicador (15)	Meta (16)	Evidencia que se observará (17)
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	1	Recuperación del crédito	Ejecución de Garantías	Falta de garantías	Interna	Procesos	Reducir	Se establecerá una instancia de revisión del Comité de Crédito que deberá revisar cada crédito y cotejar la garantía de acuerdo al tipo de crédito Se adicionará un módulo al sistema de información de créditos, para que si un crédito no tiene incorporado el número de póliza de garantía no permita cursar el crédito	Las acciones tienden a mejorar el control del riesgo que es débil estableciendo una instancia que controle al Comité de Crédito y una aplicación al sistema. También se espera disminuir la probabilidad que se concrete la falta de garantías	Jefe de Operaciones	6 meses	Porcentaje créditos sin garantía (Nº total de créditos mensuales / Nº de créditos sin garantía) * 100	mensual	- 3%	Carpeta del crédito Información del sistema Actas Comité Actas de revisión

ANEXO N° 19 - 1/2

MATRIZ DE RIESGOS ESTRATÉGICA– FORMATO TIPO

LEVANTAMIENTO DE INFORMACIÓN DE PROCESOS						RIESGOS CRÍTICOS											
Proceso Transversal	Proceso Crítico	Subproceso	Pd. (1)	Etapas	Objetivos	Descripción Riesgos Específicos	Fuente de Riesgos	Tipo de Riesgo	Señal de Alerta LA/FT/DF Asociada (2)	Cargo(s) Funcionario Relacionado (3)	Probabilidad		Impacto		Severidad del Riesgo	
											Clasif	Valor	Clasif	Valor	Clasif	Valor
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Postulación	10%	…	….	…	…	…			…	…	…	…	…	…
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Evaluación	35%	….	….	…	…	…			…	…	…	…	…	…
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Entrega de créditos	20%	…	…	..	…	…			…	…	…	…	…	…
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	35%	Cobranza	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Falta de acciones oportunas de cobranza	Interna	Procesos	SI	Jefe Depto. Cobranza	Moderado	3	Moderado	3	Alto	9
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	35%	Cobranza	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Insolvencia de los deudores	Externa	Económico	SI	Jefe Depto. Cobranza	Improbable	2	Mayores	4	Alto	8
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	35%	Cobranza	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Falta de garantías	Interna	Procesos	SI	Jefe Depto. Cobranza	Muy improbable	1	Mayores	4	Alto	4
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	35%	Ingreso fondos	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Ingreso inoportuno o incompleto de pagos	Interna	Personas	SI	Jefe Depto. Cobranza	Probable	4	Moderado	3	Alto	12
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	35%	Ingreso fondos	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Errores en la digitación de los montos	Interna	Personas	NO	–	Moderado	3	Mayores	4	Extremo	12
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	35%	Ingreso fondos	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Problemas en la transformación de la información del sistema del Servicio al SIGFE	Interna	Tecnológico	NO	-	Improbable	2	Mayores	4	Alto	8
Recursos Humanos	…	…	…	…	…	…	…	…			…	…	…	…	…	…
Capacitación	…	…	…	…	…	…	…	…			…	…	…	…	…	…
…	…	…	…	…	…	…	…	…			…	…	…	…	…	…

Continúa en la página siguiente

(1) Ponderación estratégica del subproceso en relación con los objetivos del proceso crítico y otras variables relevantes.
(2) Se debe determinar, si es posible asociar una señal de alerta de delito LA/FT/DF al riesgo identificado, si este es el caso, se debe indicar **SI**. En el caso que no sea posible asociar una señal de alerta de delito LA/FT/DF al riesgo, debe indicarse que **No**.
(3) Se debe identificar el o los cargos funcionarios que se relacionan de manera teórica y más directamente con el riesgo y/o Señal de Alerta LA/FT/DF asociada.

ANEXO N°19 - 2/2

MATRIZ DE RIESGOS ESTRATÉGICA – FORMATO TIPO

Viene de la página anterior

CONTROLES CLAVES EXISTENTES						VALOR Y CLASIFICACIÓN DE LA EXPOSICIÓN AL RIESGO Y EXPOSICIÓN AL RIESGO PONDERADA										
						Riesgo		Etapa		Subproceso				Proceso		
Descripción Controles (Norma, quién lo realiza, qué actividades desarrolla, cómo las ejecuta y cuándo y cómo se evidencia su cumplimiento)	**Cumple Elementos de Control Adecuado**	**Nivel de Efectividad**			**Valor**	**Nivel ER (3)**	**Valor ER (3)**	**Nivel ER (3)**	**Valor ER (3)**	**Nivel ER (3)**	**Valor ER (3)**	**Valor ERP (4)**	**Ranking**	**Nivel ER (3)**	**Valor ER (3)**	**Ranking**
		PD	O	A												
…	…	…	…	…	…	Mayor	6	Mayor	6	Mayor	6	0,6	3º	Media	3,8	1º
…	…	…	…	…	…	Media	3	Media	3	Media	3	1,05	2º	Media	3,8	1º
…	…	…	…	…	…	menor	2,5	menor	2,5	menor	2,5	0,5	4º	Media	3,8	1º
Qué: Aviso automático: **Cómo:** El Sistema avisa los vencimientos al Jefe de Cobranzas **Quién y Cuándo:** El Jefe finanzas revisa mensualmente las cobranzas.	SÍ	Pd	Cr	SÍ	3	Media	3	Mayor	5	medio	3,8	1,33	1º	Media	3,8	1º
Sin control.	-	-	-	-	1	No aceptable	8	Mayor	5	medio	3,8	1,33	1º	Media	3,8	1º
El Comité de crédito no puede entregar crédito sin garantía.	No	-	-	-	1	Mayor	4	Mayor	5	medio	3,8	1,33	1º	Media	3,8	1º
Qué: Validación de pagos: **Cómo y quién**: El Tesorero ingresa los pagos al sistema que autovalida los datos. Para abonos o pagos fuera de plazo se requiere autorización del superior. **Cuándo:** Mensualmente los reportes los revisa el jefe de Finanzas	SÍ	Pe	Pr	SÍ	5	Menor	2,4	Menor	2,5	medio	3,8	1,33	1º	Media	3,8	1º
Qué: Validación de pagos **Cómo:** Se ingresan los pagos al sistema que autovalida los datos. Para abonos o pagos fuera de plazo se requiere autorización del superior. **Quien:** El tesorero. **Cuándo:** Mensualmente los reportes los revisa el jefe de Finanzas.	SÍ	Pe	Pr	SÍ	5	Menor	2,4	Menor	2,5	medio	3,8	1,33	1º	Media	3,8	1º
Qué: Visación transformación de datos. **Cómo:** Se revisa la transformación de todos los datos **Quién:** El Jefe de Finanzas **Cuándo**: Se revisa la transformación antes de remitirse los datos al exterior.	SÍ	Pd	Cr	M	3	Menor	2,7	Menor	2,5	medio	3,8	1,33	1º	Media	3,8	1º
…	…	…	…	…	…	…	…	…	…	…	…	…	….	…	….	2°
…	…	…	…	…	…	…	…	…	…	…	…	…	….	…	….	3°
…	…	…	…	…	…	…	…	…	…	…	…	…	….	….	….	….

(3) ER= Nivel de Exposición al Riesgo.
(4) ERP= Nivel de Exposición al Riesgo Ponderada.

ANEXO Nº 20

EJEMPLO DE LEVANTAMIENTO DE INFORMACIÓN DE UN PROCESO

A continuación, se presenta un ejemplo de levantamiento de información del subproceso "Compra de bienes y servicios", que forma parte del proceso crítico denominado "Compras y Abastecimiento" en una entidad ficticia.

Con la finalidad de lograr una mejor comprensión del ejemplo, se hará un análisis detallado de los riesgos y controles para las etapas de Selección y Adjudicación.

Cuadro N° 1: Levantamiento de Información de cada Proceso

Proceso	Subprocesos	Etapas	Entradas del subproceso o proceso	Salidas del subproceso o proceso
Compras y abastecimiento	Planificación operativa anual de compras.	....	....	....
		....	....	....
		....	....	....
	Compra de bienes y servicios.	Definición naturaleza del proceso.	Plan Operativo de compras.	Bienes y servicios (insumos) de calidad que satisfagan los requerimientos para producción de la organización gubernamental.
		Confección y publicación de Bases.		
		Selección.		
		Adjudicación.		
	Recepción y evaluación de bienes y servicios adquiridos.	....	....	....
		....	....	....
		....	....	....
	....	....	....	....
	....	....	....	....

Cuadro N° 2: Levantamiento de Información de las Etapas Selección y Adjudicación

Etapas	Objetivo operativo de la etapa	Actividades de la etapa		Responsables
		De gestión	De control	
Etapa Definición de la naturaleza del proceso de compras a utilizar (convenio marco, licitación pública, privada, trato directo).	Definir de acuerdo a las características del bien o servicio a comprar, la forma de adquirirlo en el mercado, de conformidad a la normativa de compras.	1.- El Comité de Compras, en base a lo establecido en el Plan de Compras define cómo se realizará cada adquisición (licitación pública, privada o trato directo).		Comité de Compras
			2.- El Jefe de Finanzas y de la Unidad Jurídica visan la definición del Comité.	Jefe Finanzas Jefe Unidad Jurídica

Etapas	Objetivo operativo de la etapa	Actividades de la etapa		Responsables
		De gestión	De control	
Etapa Confección y publicación de bases.	Establecer formalmente bases administrativas y técnicas adecuadas a la especificación técnica de lo requerido y que respeten la transparencia e igualdad de los oferentes.	1.- Se realiza la definición de especificaciones técnicas (características, plazos, volúmenes, calidades, etc.).		Encargado de especificaciones técnicas de compras
			2.-Validan y visan la definición técnica.	Jefe de Abastecimiento y Jefe Unidad solicitante
		3.- Confeccionar bases de licitación oportunas y completas (de acuerdo con el procedimiento formal de la organización gubernamental).		Jefe de Finanzas Jefe de la Unidad Jurídica
			4.- Aprobación oportuna de las Bases de Licitación.	Jefe de la Unidad Jurídica Jefe de Servicio
		5.- Publicar en diarios en forma completa, oportuna y legal		Jefe de Finanzas
		6.- Aclarar en forma completa e igualitaria las dudas de los oferentes.		Jefe de Finanzas Jefe de la Unidad Jurídica
			7.- Verificación que todas las compras cuenten con una carpeta con antecedentes de licitación, bases y publicación.	Encargado de análisis del área de compras
Etapa Selección	Realizar una selección transparente, garantizando la participación igualitaria de los oferentes.	**Licitaciones privada y pública**		
		1.- Recepción de todas las ofertas remitidas (igualdad de oferentes).		Comité de Compras
			2.- Chequeo automatizado de cumplimiento de Plazos.	Encargado Sistema de Información de Compras
		3.- Apertura de acuerdo a la normativa de compras, a través del sistema de Chilecompras.		Comité de Compras Encargado del Sistema de Información de Compras
			4.- Participación de Ministro de Fe en la apertura.	Funcionario de la Unidad Jurídica
			5.- Confección de acta de recepción de ofertas, especificando día y hora de las ofertas recibidas.	Encargado Of. de Partes Jefe de Finanzas
			6.- Confección de acta de apertura con todos los participantes que cumplen requisitos.	Comité de Compras Ministro de Fe

Etapas	Objetivo operativo de la etapa	Actividades de la etapa		Responsables
		De gestión	De control	
			7.- Entrega de reportes del sistema al comité de compras.	Encargado del sistema de compras y supervisor
		Compra directa		
		1.- Se designan cotizadores al interior de la organización gubernamental.		Jefe de Finanzas y Comité de Compras
			2.- Cruces de datos entre funcionarios participantes del proceso de compras y proveedores.	Jefe de Abastecimiento
		3.- Obtención de a lo menos tres cotizaciones en el caso de trato directo.		Cotizadores designados.
Etapa Adjudicación	Adjudicar la compra al oferente que presente la oferta más conveniente para la organización.		1.- Evaluación técnica, de acuerdo a criterios previos y objetivos dispuestos en procedimiento.	Comité de Compras.
		2.- Se levanta un acta de proposición de adjudicación con el fundamento de la decisión según desarrollo del proceso.		Comité de Compras.
			3.- Revisión de la adjudicación para determinar su conformidad al procedimiento y Bases.	Jefe de Abastecimiento
			4.- Revisión de la consistencia y legalidad del proceso.	Jefe de la Unidad Jurídica
			5.- Se verifica que el proveedor adjudicado no tengan inhabilidades respecto de funcionarios de la organización gubernamental y cumplan obligaciones laborales.	Jefe de Finanzas. Jefe de Recursos Humanos.
			6.- Visación de la adjudicación	Jefe de la Unidad Jurídica
		7.- Aprobación de Adjudicación		Jefe de Servicio o delegatario.

Cuadro N° 3: Ejemplo de Identificación de Riesgos Asociados a las Actividades Realizadas para Lograr los Objetivos Operativos de las Etapas Selección y Adjudicación

Etapa	Objetivo operativo de la etapa	Actividades de la etapa	Riesgos asociados a la realización de las actividades
Etapa…	…	…	…
Etapa…	…	…	…
Etapa Selección	Realizar una selección transparente, garantizando la participación igualitaria de los oferentes.	**Licitaciones privada y pública**	
		1.- Recepción de todas las ofertas remitidas. (Igualdad de oferentes).	Recepción de ofertas fuera de plazo.
			Recepción de ofertas en forma distinta a la señalada en las bases.
		2.- Apertura de acuerdo a la normativa de compras a través del sistema de ChileCompra.	La apertura no se realiza a través del sistema y no se cumple el procedimiento aprobado.
			La apertura se realiza en día y hora distinta al establecido en las bases.
		3.- Participación de Ministro de Fe en la apertura.	Ministro de Fe con incompatibilidades.
		4.- Confección de acta de recepción de ofertas, especificando día y hora de las ofertas recibidas.	En caso de recepción en papel, no se confecciona Acta de recepción o ésta es incompleta o errónea.
		5.- Confección de acta de apertura con todos los participantes que cumplen con los requisitos.	Las actas se firman posteriormente por las personas que no asisten a la apertura.
		6.- Entrega de reportes del sistema al comité de compras.	No se entregan reportes en forma oportuna o tienen datos erróneos.
		Compra directa	
		1.- Se designan cotizadores al interior de la organización gubernamental.	Designación de cotizadores con incompatibilidades.
		2.- Cruces de datos entre funcionarios participantes del proceso de compras y proveedores	No se realizan cruces de datos entre funcionarios y proveedores
			No se cuenta con la información para cruzar datos
		3.- Obtención de a lo menos tres cotizaciones en el caso de trato directo.	Falta de tres cotizaciones para trato directo sin fundamento.
			Cotizaciones manejadas para favorecer a un proveedor.
Etapa Adjudicación	Adjudicar la compra al oferente que presente la oferta más conveniente para la organización.	1.- Evaluación técnica, de acuerdo a criterios previos y objetivos dispuestos en procedimientos.	Errores en evaluación técnica.
			Adjudicación con criterios distintos a los establecidos en la ley, las bases y los procedimientos.
		2.- Se levanta un acta de proposición de adjudicación con el fundamento de la decisión según desarrollo del proceso.	Adjudicación no es consistente con el proceso de evaluación.
		3.- Revisión de la adjudicación para determinar su conformidad al procedimiento y Bases.	La adjudicación no es consisten con las Bases o con el procedimiento establecido.
		4.- Revisión de la consistencia y legalidad del proceso.	El proceso presenta deficiencias legales de forma o fondo
		5.- Se verifica que el proveedor adjudicado no tenga inhabilidades	Inexistencia de antecedentes para realizar la verificación

Etapa	Objetivo operativo de la etapa	Actividades de la etapa	Riesgos asociados a la realización de las actividades
		respecto de funcionarios de la organización gubernamental y cumplan obligaciones laborales.	Funcionarios que realizan verificación no cuentan con las competencias necesarias.
		6.- Visación de Adjudicación.	No se cuenta con todos los antecedentes para visar la operación.
		7.- Aprobación de la adjudicación.	El funcionario que aprueba no tiene las facultades delegadas

Cuadro N° 4: Ejemplo de Identificación de Riesgos Asociados a las Entradas del Subproceso o Proceso

Etapas que afecta	Objetivo operativo de la etapa	Entradas al subproceso o proceso	Riesgos asociados a las entradas del subproceso o proceso
Etapa Selección	Realizar una selección transparente, garantizando la participación igualitaria de los oferentes.	Plan Operativo de Compras.	1.- Deficiencias técnicas en la formulación del Plan. El Plan no representa las necesidades de compra de la organización gubernamental. 2.- Falta de aprobación o autorización del Plan. ...

Cuadro N° 5: Identificación de Controles Mitigantes para Cada Riesgo Operativo Asociado a las Actividades Realizadas en las Etapas de Selección y Adjudicación

Etapas	Riesgos asociados a la realización de las actividades	Controles operativos mitigantes clave	Responsables
Etapa Selección	**Licitación privada y pública**		
	Recepción de ofertas fuera de plazo. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Chequeo automatizado de plazo. **Cómo**: El sistema de información ADBG, contiene un algoritmo que controla y chequea la hora y la fecha de la apertura. **Cuándo**: Lo anterior se realiza por cada apertura para todas las ofertas. **Quién:** Este chequeo lo hace el Encargado de Sistema de Información de Compras.	Encargado Sistema de Información de Compras
		Qué: Chequeo manual de plazo y confección de Acta de Recepción. **Cómo:** En caso de ofertas no recibidas por el sistema, el encargado de la Oficina de Partes, levanta un acta con individualización de día y hora de las ofertas recibidas, que es visada por el Jefe de Finanzas. **Cuándo:** Esto se hace en cada licitación para todos los oferentes. **Quién:** Encargado oficina de Partes / Jefe de Finanzas.	Encargado Oficina de Partes Jefe de Finanzas
	Recepción de ofertas en forma distinta a la señalada en las bases. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué**: Chequeo de recepción y confección de Acta de Apertura. **Cómo**: El comité de compras controla el proceso de recepción y levanta un Acta de todas las ofertas recibidas, con participación de un Ministro de Fe. El sistema o el encargado (si son extra sistema) mantiene los antecedentes de las consultas y respuestas a los oferentes, con fecha. **Cuándo:** Esto se hace en cada licitación para todos los oferentes. **Quién:** Comité de Compras / Encargado Sistema de Compras / Ministro de Fe.	Comité de Compras Ministro de Fe Encargado del Sistema de Compras
	La apertura no se realiza a través del sistema y no se cumple el procedimiento aprobado. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Revisión uso del sistema. **Cómo:** La recepción y apertura de las ofertas deben realizarse a través del portal de Chilecompras. Este procedimiento es verificado diariamente, por el Encargado del Sistema de Información mediante un reporte que se emite en el área abastecimiento, visado por el supervisor **Cuándo:** Diariamente. **Quién:** Encargado sistema / supervisor.	Encargado de Sistema de Información y su supervisor
	La apertura se realiza en día y hora distinta al establecido en las bases. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Verificación de la apertura. **Cómo:** Si es una apertura extra sistema, se debe realizar en dependencias de la organización gubernamental con la asistencia de un Ministro de Fe, abogado de la Unidad Jurídica, que certifica que el día y hora corresponde a las Bases. **Cuándo:** Esto se hace en cada licitación para todos los oferentes. **Quién:** Funcionario unidad jurídica como Ministro de Fe.	Funcionario de la Unidad Jurídica
	Ministro de Fe con incompatibilidades. Señal de Alerta LA/FT/DF Asociada: Sí.	Sin control	-

Etapas	Riesgos asociados a la realización de las actividades	Controles operativos mitigantes clave	Responsables
	Las actas se firman posteriormente por las personas que no asisten a la apertura. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Chequeo de asistencia y visto bueno. **Cómo:** En el caso de apertura en soporte de papel, existe un Acta elaborada por el Comité de Compras que da cuenta de la apertura firmada por la entidad y los oferentes presentes en la apertura, con la asistencia de un Ministro de Fe. **Cuándo:** Esto se hace en cada apertura en soporte papel para todos los oferentes. **Quién**: Comité de Compras / Ministro de Fe.	Comité de Compras Ministro de Fe
	No se entregan reportes en forma oportuna o tienen datos erróneos. Señal de Alerta LA/FT/DF Asociada: N/A.	**Qué:** Revisión de reportes y autorización. **Cómo:** La información se revisa por el Encargado del Sistema de Compras y se autoriza por el supervisor. **Cuándo**: Cada vez que se emite un reporte por el sistema, y al menos mensualmente. **Quién:** Supervisor del Sistema de Información / Encargado Sistema de Compras.	Encargado Sistema de Compras Supervisor
	Compra directa		
	Designación de cotizadores con incompatibilidades. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Cruce de datos. **Cómo:** Se realiza un cruce de datos de los funcionarios involucrados en el proceso de compras y los con poder de decisión y los proveedores frecuentes de la organización gubernamental. **Cuándo:** Semestralmente. **Quién:** Jefe de Recursos Humanos.	Jefe de Recursos Humanos
	Falta de tres cotizaciones para trato directo sin fundamento. Señal de Alerta LA/FT/DF Asociada: Sí.	Sin control	-
	Cotizaciones manejadas para favorecer a proveedor. Señal de Alerta LA/FT/DF Asociada: Sí.	Sin control	-
Etapa Adjudicación	Errores en la evaluación técnica. Señal de Alerta LA/FT/DF Asociada: N/A	Qué: Revisión de la evaluación y visto bueno. Cómo: Se analizan las ofertas a través de los requisitos establecidos en la Ley, las bases y el procedimiento, emitiendo un informe técnico, con visto bueno del Jefe de Abastecimiento. Cuándo: Esto se realiza por cada proceso de licitación. Quién: El Comité de Compras y Jefe de Abastecimiento.	Comité de Compras Jefe de Abastecimiento
	Adjudicación con criterios distintos a los establecidos en la Ley y las bases. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Examen de criterios y aplicación de check list. **Cómo:** Se revisa cada adjudicación en contra de los requisitos de las bases (check list) y pone visto bueno sólo si se cumplen todos los requisitos. **Cuándo:** Esto se realiza por cada proceso de licitación que se adjudica. **Quién**: Jefe de Abastecimiento.	Jefe de Abastecimiento

Etapas	Riesgos asociados a la realización de las actividades	Controles operativos mitigantes clave	Responsables
	Adjudicación no es consistente con el proceso de evaluación. Señal de Alerta LA/FT/DF Asociada: SÍ.	**Qué:** Chequeo de consistencia. **Cómo:** Se revisa y se da visto bueno a la resolución de adjudicación antes de la firma del Jefe Superior y revisa la consistencia del proceso. **Cuándo:** Cada resolución es revisada y chequeada. **Quién:** Unidad Jurídica.	Jefe de la Unidad Jurídica
	Inexistencia de antecedentes para realizar la verificación. Señal de Alerta LA/FT/DF Asociada: N/A.	**Qué:** Examen a las competencias y herramientas de verificación. **Cómo**: Hay un encargado de mantener y conseguir las herramientas necesarias para realizar los cruces de datos (bases de datos públicas, declaraciones de interés y otros antecedentes) y de capacitar a los funcionarios que realizan esta labor en el manejo de bases de datos y consultas, y en el manejo de la normativa y jurisprudencia administrativa asociadas a temas de probidad. **Cuándo**: El examen de herramientas y la determinación de competencias se hace al menos una vez al año. **Quién:** Jefe de Recursos Humanos	Jefe de Finanzas
	Funcionarios que realizan verificación no cuentan con las competencias necesarias. Señal de Alerta LA/FT/DF Asociada: N/A.		Jefe de Recursos Humanos
	No se cuenta con todos los antecedentes para visar la operación. Señal de Alerta LA/FT/DF Asociada: Sí.	Sin control	-
	El funcionario que aprueba no tiene las facultades delegadas. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Chequeo de facultades. **Cómo:** se visa la aprobación, revisando los aspectos de forma y fondo y las atribuciones del firmante. **Cuándo:** Cada adjudicación y resolución que la apruebe es revisada por la unidad Jurídica de la organización gubernamental. **Quién:** La Unidad Jurídica previa a la aprobación.	Jefe Unidad Jurídica

Cuadro N° 6: Identificación de Controles Mitigantes para Cada Riesgo Operativo Identificado Asociado a las Entradas del Subproceso o Proceso

Etapa que afecta	Riesgos asociados a las entradas del subproceso o proceso	Controles operativos mitigantes claves	Responsables
Etapa Selección	1.- Deficiencias técnicas en la formulación del Plan. El Plan no representa las necesidades de la organización gubernamental. Señal de Alerta LA/FT/DF Asociada: N/A.	**Qué**: Revisión del Plan. **Cómo:** Existe información en la organización gubernamental histórica acerca del gasto y adquisiciones de la Organización Gubernamental que maneja el Jefe de Finanzas. **Cuándo:** Cada Unidad hace llegar a la Comisión de Planificación, al 15 de noviembre de cada año, un programa operativo anual con los requerimientos y necesidades para el próximo año, calendarizadas y presupuestadas. **Quién**: Jefe de Finanzas.	Jefe de Finanzas Jefe de Cada Unidad Operativa
		Qué: Participación en distintos niveles. **Cómo**: Existen procedimientos formales con participación de las diversas instancias para definir el Plan (Comisión de Planificación), que se revisa y aprueba anualmente por el Jefe de Servicio previo informe de la Comisión de Planificación y del Jefe de Finanzas. **Cuándo:** Anualmente. **Quién:** Comisión de Planificación / Jefe de Servicio.	Jefe de Servicio Comisión de Planificación
	2.- Falta de aprobación o autorización del Plan. Señal de Alerta LA/FT/DF Asociada: Sí.	**Qué:** Aprobación del Plan. **Cómo:** Se revisa el Plan y se consideran los análisis de la Comisión de Planificación y del Jefe de Finanzas para aprobar, rechazar o modificar el Plan propuesto. **Cuándo:** Hasta el 30 de diciembre de cada año. **Quién:** Jefe de Servicio.	Jefe de Servicio Comisión de Planificación

CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Documentos Técnicos del CAIGG

A cerca de los Documentos Técnicos del CAIGG (DT)

Los Documentos Técnicos del CAIGG constituyen orientaciones especializadas destinadas a fortalecer y apoyar el ejercicio de la auditoría interna en el sector público. Abordan un conjunto amplio y estratégico de materias, entre ellas la gestión de riesgos, la prevención de la corrupción, la probidad administrativa, la auditoría interna, el gobierno corporativo, el control interno y la gestión de riesgos financieros, contribuyendo a la mejora continua y a la alineación con buenas prácticas nacionales e internacionales.

Área de Estudios del Consejo de Auditoría Interna General de Gobierno