Ministerio Secretaría General de la Presidencia

Gobierno de Chile

DOCUMENTO TÉCNICO N° 70
Versión 0.3

IMPLANTACIÓN, MANTENCIÓN Y ACTUALIZACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS EN EL SECTOR PÚBLICO

Este documento tiene como principal objetivo facilitar a las organizaciones gubernamentales, la implementación y cumplimiento del Proceso de Gestión de Riesgos, así como su mantención y mejora continua. El enfoque técnico está basado principalmente en la Norma Chilena NCh-ISO 31000:2018, Gestión del Riesgo - Principios y Orientaciones, y en menor medida en el Marco de Gestión de Riesgos Corporativos ERM – COSO II.

CONSEJO DE AUDITORIA INTERNA GENERAL DE GOBIERNO

CAIGG

Ministerio Secretaría General de la Presidencia

SEPTIEMBRE 2022

TABLA DE CONTENIDOS

MATERIAS	PÁGINA
PRESENTACIÓN	3
I.- INTRODUCCIÓN	4
II.- OBJETIVO GENERAL DEL DOCUMENTO	6
III.- RELACIÓN CON EL ASEGURAMIENTO	6
IV.- MARCO METODOLÓGICO PARA EL PROCESO DE GESTIÓN DE RIESGOS	6
V.- PROCESO DE GESTIÓN DE RIESGOS	7
1.- Conceptos Generales sobre Riesgos	7
2.- Conceptos Generales sobre Gestión de Riesgos	7
3.- Componentes de la Norma NCH-ISO 31000:2018	9
4.- Relación entre los Componente de la Norma NCh-ISO 31000:2018	16
VI.- CONCEPTOS Y ELEMENTOS A INCORPORAR PARA EL MARCO DE TRABAJO Y PROCESO DE GESTIÓN DE RIESGOS EN LAS ORGANIZACIONES GUBERNAMENTALES	17
A.- Marco de Trabajo de la Gestión de Riesgos	17
B.- Mantención y Mejoramiento del Proceso de Gestión de Riesgos	17
1.- Fase Alcance, Contexto, Criterio	17
2.- Fase Identificación del Riesgo	36
3.- Fase Análisis del Riesgo	41
4.- Fase Valoración del Riesgo	44
5.- Fase Tratamiento del Riesgo	47
6.- Fase Seguimiento y Revisión	52
7.- Fase Comunicación y Consulta	54
8.- Fase Registro e Informe	59
C.- Reportes del Proceso de Gestión de Riesgos al Consejo de Auditoría Interna	61
VII.- BIBLIOGRAFÍA	62

ANEXO Nº 1: EJEMPLO: MODELO DE POLÍTICA DE GESTIÓN DE RIESGOS 63

ANEXO Nº 2: EJEMPLO: MODELO DE DEFINICIÓN DE ROLES Y RESPONSABILIDADES 65

ANEXO Nº 3: ROL DE LA AUDITORÍA INTERNA EN EL PROCESO DE GESTIÓN DE RIESGOS EN EL SECTOR GUBERNAMENTAL 68

ANEXO Nº 4: GUÍA BÁSICA PARA EL LEVANTAMIENTO DE INFORMACIÓN DE LOS PROCESOS Y MODELAMIENTO DE RIESGOS 70

ANEXO Nº 5: CRITERIOS: TABLAS DE VALUACIÓN PARA CONSTRUIR LA MATRIZ DE RIESGOS -APETITO DEL RIESGO- 73

ANEXO Nº 6: EJEMPLO DE LEVANTAMIENTO DE INFORMACIÓN DE UN PROCESO 79

ANEXO Nº 7: EJEMPLOS DE TÉCNICAS DE EVALUACIÓN DE RIESGOS Y OPORTUNIDADES 88

ANEXO Nº 8: EJEMPLOS DE RIESGOS Y CONTROLES RELACIONADOS CON EL GOBIERNO ELECTRÓNICO 91

ANEXO Nº 9: CONCEPTOS GENERALES SOBRE REQUISITOS BÁSICOS DE CONTROL ADECUADO CONSIDERADOS EN EL MODELO 94

ANEXO Nº 10: EJEMPLO: INFORMACIÓN PARA EL TRATAMIENTO DE RIESGOS 108

ANEXO Nº 11: MATRIZ DE RIESGOS ESTRATÉGICA – FORMATO TIPO 109

ANEXO N° 12: CONCEPTOS SOBRE DELITOS DE LAVADO DE ACTIVOS (LA), FINANCIAMIENTO DEL TERRORISMO (FT) Y DELITOS FUNCIONARIOS (DF) 111

ANEXO N°13: EJEMPLOS DE SEÑALES DE ALERTA GENÉRICAS PARA DELITOS LA/FT/DF 115

ANEXO N° 14: SEÑALES DE ALERTA LA/FT/DF NO ASOCIADAS CON LOS RIESGOS INCLUIDOS EN LA MATRIZ DE RIESGOS ESTRATÉGICA 125

PRESENTACIÓN

Como una de las iniciativas tendientes al fortalecimiento de la Auditoría Interna considerado en el Programa de Gobierno de S.E. el Presidente de la República, Gabriel Boric Font; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, gestión de riesgos y gobernanza, tiene el rol de promover la mejora continua de la función de auditoría interna gubernamental, y entregar recursos a la red de auditores para la generación de competencias y perfeccionamiento técnico de su trabajo, considerando las últimas tendencias de auditoría interna y las mejores prácticas aceptadas a nivel nacional e internacional.

En este ámbito, se pone a disposición de la Administración del Estado, el Documento Técnico N° 70, versión 0.3 denominado "Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público". Esta versión del documento que ha sido actualizado con las últimas versiones de las normas y marcos aceptados sobre gestión de riesgos está concebido para ser una directriz a ser aplicada en el Estado, en la implementación, mantención y mejora continua del Proceso de Gestión de Riesgos.

Santiago, septiembre 2022.

Daniella Caldana Fulss
Auditora General de Gobierno

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, descrito como el sistema mediante el cual las entidades son dirigidas y controladas para contribuir a su efectividad y desempeño. Su fin último es contribuir a la maximización del valor de las compañías, en un horizonte de largo plazo.[1] 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 del mismo; 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

[1] Gobierno Corporativo en Chile después de la Ley de OPAS, Teodoro Wigodski S1, Franco Zúñiga G, Departamento de Ingeniería Industrial. Universidad de Chile.

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 CAIGG, servirán para retroalimentar el proceso.

En el presente documento se ha consolidado toda la información disponible referida al Proceso de Gestión de Riesgos en el Sector Gubernamental, estableciéndose la siguiente estructura:

- Como punto I esta introducción; en el punto II se señala el objetivo general del documento; en el punto III, la relación con la Auditoría de Aseguramiento del Proceso de Gestión de Riesgos; en el punto IV, el marco metodológico para el Proceso de Gestión de Riesgos bajo NCh-ISO 31000:2018; en el punto V, se establecen conceptos básicos y fundamentales de la Gestión de Riesgos; en el punto VI se señala el análisis de las fases del Proceso de Gestión de Riesgos que deben ser aplicadas por las organizaciones gubernamentales; también se señala en el punto VI, la necesidad que las organizaciones gubernamentales envíen al CAIGG los reportes derivados del Proceso de Gestión de Riesgos en los términos, plazos y formatos que esta entidad comunique oportunamente, y en el punto VII, se presenta la Bibliografía que sustenta el presente documento.

- Finalmente, se adjuntan 14 anexos: en el Anexo Nº 1, se incorpora un ejemplo ilustrativo de política de gestión de riesgos; en el Anexo Nº 2 un ejemplo de asignación de roles y responsabilidades; en el Anexo Nº 3 la descripción del rol de la auditoría interna en el Proceso de Gestión de Riesgos en el sector gubernamental; en el Anexo Nº 4 se entrega una guía básica para el levantamiento de procesos y modelamiento de riesgos; el Anexo Nº 5 establece las tablas de valuación para riesgos, controles y exposición; el Anexo Nº 6 entrega un ejemplo de levantamiento información de un proceso; el Anexo Nº 7 enuncia técnicas de evaluación de riesgos y oportunidades, bajo NCh-ISO 31010:2020; el Anexo Nº 8 entrega un ejemplo de riesgos y controles relacionados con el Gobierno Electrónico; el Anexo Nº 9 define los conceptos generales sobre requisitos básicos de control adecuado considerados en el modelo; el Anexo Nº 10 presenta un ejemplo de plan de tratamiento de riesgos con estrategias, acciones e indicadores, el Anexo Nº 11 se acompaña un ejemplo de Matriz de Riesgos Estratégica construida con la metodología descrita en este documento; en el Anexo N° 12 se entregan conceptos y definiciones sobre delitos de lavado de activos (LA), financiamiento del terrorismo (FT) y delitos funcionarios (DF); el Anexo N°13 contiene ejemplos de señales de alerta genéricas para delitos LA/FT/DF y, por último en el Anexo N° 14, se incluye una estructura para levantar información sobre señales de alerta de delitos LA/FT/DF no asociadas con los riesgos incluidos en la Matriz de Riesgos Estratégica.

Hay que relevar, que cada organización gubernamental debe tener implementado un Proceso de Gestión de Riesgos que sea útil para identificar y gestionar aquellos eventos que puedan afectar el logro de sus objetivos estratégicos y misión institucional. Para ello, deben aplicarse todas las fases que se definen en el presente documento técnico, con la finalidad de tener una gestión de riesgos sólida. Periódicamente, el CAIGG podrá solicitar algunos reportes derivados del Proceso de Gestión de Riesgos, pero para obtener estos reportes la organización gubernamental debe ejecutar la metodología contenida en la presente directriz, para conseguir por una parte un Proceso de Gestión de Riesgos robusto funcionando en la organización gubernamental y por otra, reportes de calidad, que entreguen información adecuada para la Presidencia de la República, para la coordinación y gestión adecuada de los diversos organismos del Gobierno.

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:

- Dar cumplimiento a las directrices que, sobre la materia, formule el CAIGG, de acuerdo con lo definido en el Decreto Supremo N° 12 del año 97.
- 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.- RELACIÓN CON EL ASEGURAMIENTO

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. 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.- MARCO METODOLÓGICO PARA EL PROCESO DE GESTIÓN DE RIESGOS

El modelo metodológico para la Gestión de Riesgos en las organizaciones gubernamentales estará 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[2].
A contar del año 2016 se han incorporado elementos conceptuales y metodológicos para identificar y analizar señales de alerta para delitos de lavado de activos (LA), financiamiento del terrorismo (FT) y delitos funcionarios (DF).

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.

V.- PROCESO DE GESTIÓN DE RIESGOS

1.- Conceptos Generales sobre Riesgos

La Norma NCh-ISO Guía 73:2012 define riesgo como el efecto de la incertidumbre sobre los objetivos y destaca que, con frecuencia el riesgo se caracteriza por referencia a potenciales eventos y consecuencias, o a una combinación de ambos. Por su parte, en el Marco Integrado de Control Interno – COSO I (Versión 2013) el riesgo se define como la posibilidad (probabilidad) de que un acontecimiento ocurra y afecte (consecuencia o impacto) negativamente a la consecución de los objetivos. La evaluación del riesgo implica un proceso dinámico e iterativo para identificar y evaluar los riesgos de cara a la consecución de los objetivos. Dichos riesgos deben evaluarse en relación a unos niveles preestablecidos de tolerancia. De este modo, la evaluación de riesgos constituye la base para determinar cómo se gestionarán. Una condición previa a dicha evaluación es el establecimiento de objetivos asociados a los diferentes niveles de la entidad.

El Marco Integrado de Control Interno – COSO I (Versión 2013) incluye adicionalmente a los atributos clásicos de evaluación de riesgos: probabilidad y consecuencia o impacto, dos nuevos elementos para tener en cuenta; específicamente se incluye el concepto de velocidad y el de persistencia de los riesgos:

- La velocidad de riesgo se refiere a la rapidez con la que impacta un riesgo en la entidad, es decir, se refiere al ritmo con el que se espera que la entidad experimente el impacto.
- La persistencia de un riesgo hace referencia a la duración del impacto en la entidad después de que el riesgo se haya materializado.

En forma complementaria, el documento *Risk Assessment in Practice Thought Paper,* de la organización COSO[3] emitido el año 2012, incluye en la evaluación del riesgo los elementos de velocidad de ocurrencia y vulnerabilidad, cuyo concepto corresponde a la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que haya ocurrido un desastre.

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

[2] Marco Gestión de Riesgos Empresariales COSO ERM, Modelo de Capacidad GRC - OCEG, entre otros.
[3] www.coso.org

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, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto del alcance 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.[4]

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[5]. 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.[6]

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.

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.

[4] 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.
[5] NCh-ISO 31000:2018.
[6] Marco Gestión de Riesgos Empresariales COSO ERM.

- Genera mayor 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 del 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[7]; el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad[8] o la cantidad y tipo de riesgo que una organización desea retener o perseguir[9]. 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 es el nivel aceptable de la variación alrededor del 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 cantidad 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 soportar en la persecución de sus objetivos.

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 al riesgo mayor que otras para alcanzar sus objetivos (por ejemplo, las entidades de apoyo social potencialmente son más riesgosas por el tipo de usuario vulnerable), así como cada una de estas tendrá niveles distintos de tolerancia y capacidad de riesgos.

3.- 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.

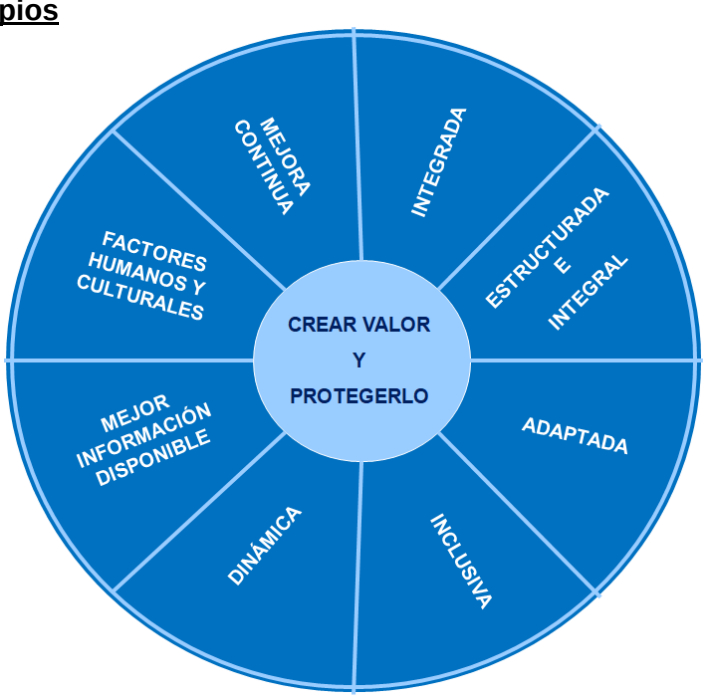
La gestión de riesgos puede aplicarse a toda una organización, en sus áreas y niveles, en cualquier momento, así como a las funciones específicas, proyectos y actividades.

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

3.1.- PRINCIPIOS

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 principios siguientes:

Gráfica N° 1: Principios



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.

3.2.- 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 Gráfica N° 2 a continuación.

Gráfica 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:

a.- 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.

b.- 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.

c.- 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.

d.- 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.

e.- 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.

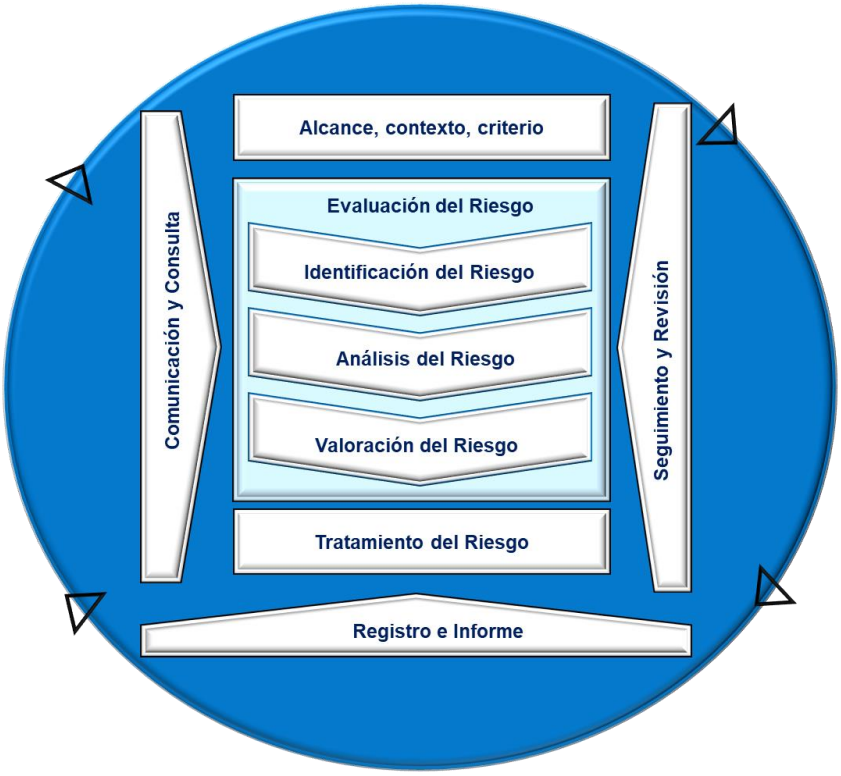
f.- Mejora

La entidad debería mejorar continuamente la idoneidad, adecuación y eficacia del marco de referencia de la gestión del riesgo y la manera en la que se integra el proceso de la gestión del riesgo.

3.3.- 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.

Gráfica 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.

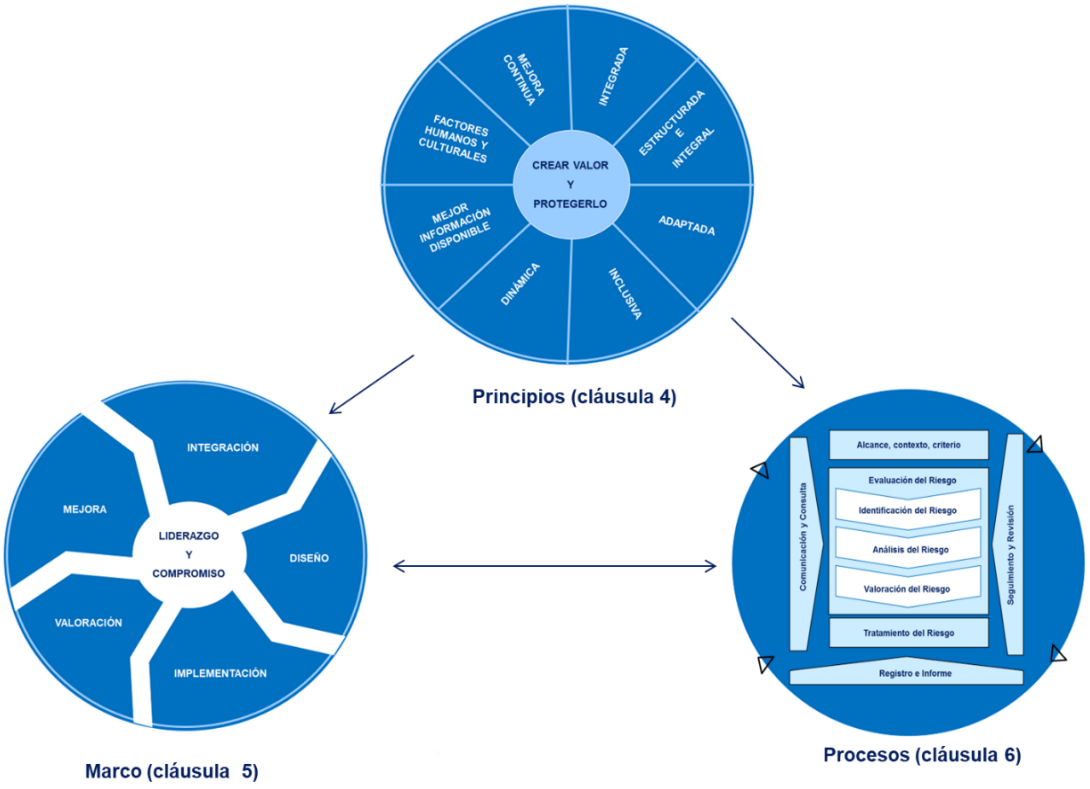
- **Seguimiento y Revisión:** Como parte del proceso de gestión del riesgo, los riesgos y los controles se deben monitorear y revisar de manera regular. Comprende definir y utilizar mecanismos para la verificación, supervisión, observación crítica o determinación del estado de los riesgos y controles 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.

4. 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 a como se presenta en la Grafica 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.

Gráfica 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.

VI.- CONCEPTOS Y ELEMENTOS A INCORPORAR PARA EL MARCO DE TRABAJO Y PROCESO DE GESTIÓN DE RIESGOS EN LAS ORGANIZACIONES GUBERNAMENTALES

En los párrafos siguientes, se revisará cada una de las fases del Marco de Trabajo y del Proceso de Gestión de Riesgos:

A. MARCO DE TRABAJO DE LA GESTIÓN DE RIESGOS

Desde el año 2014, las actividades comprendidas en cada elemento del Marco de Trabajo de la Gestión del Riesgo, se han venido implementando y actualizando en forma paralela y complementaria con las actividades de implantación del Proceso de Gestión de Riesgos principalmente en base a la NCh-ISO 31000:2012. A contar del año 2022 se utiliza la Norma NCh-ISO 31000:2018, ya que continúa proporcionando directrices globales que pueden adaptarse a cualquier organización y a su contexto, mediante un enfoque común que contribuye a gestionar cualquier tipo de riesgo en el sector público, entre otras industrias.

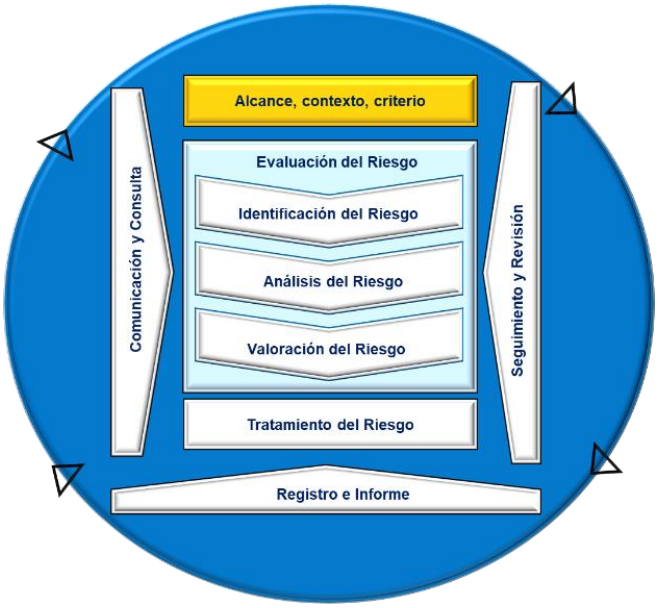
Para efectos metodológicos, el presente documento desarrolla en primer lugar la Fase: Alcance, Contextos, Criterios.

B. MANTENCIÓN Y MEJORAMIENTO DEL PROCESO DE GESTIÓN DE RIESGOS

1.- FASE ALCANCE, CONTEXTO, CRITERIO

En esta fase genérica, se contempla el establecimiento del alcance, el criterio y el contexto estratégico, organizacional y de gestión en los cuales tendrá lugar el Proceso de Gestión de Riesgos. Incluye el contexto interno, el externo y el contexto de gestión de riesgos.

Gráfica N° 5: Fase Alcance, Contextos, Criterios



Fuente: NCh-ISO 31000:2018 – INN

1.1.- Contexto Interno y Externo

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.

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.

i) 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[10]. 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 organizacionales, estableciendo responsables y plazo de las comunicaciones. En Anexo Nº 1 se entrega un ejemplo de política de gestión de riesgos.

[10] NCH-ISO GUIA 73:2012

Acciones a Desarrollar Periódicamente

En esta fase debe definirse la política de gestión de riesgos y aprobarse por el Jefe de Servicio mediante resolución exenta o documento equivalente. En el caso de estar dictada, debe revisarse, 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.

ii) 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 2, 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 3 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[11].

Acciones a Desarrollar Periódicamente

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.

iii) 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 ha sido confeccionado y remitido por el CAIGG a todas las organizaciones del Sector Público para que lo utilicen.

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

Acciones a Desarrollar Periódicamente

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.

1.2.- Alcance y Contexto de Gestión de Riesgo

Para establecer el contexto de gestión debe constituirse y definirse el alcance de aplicación del análisis de riesgos de acuerdo con la estructura organizacional.

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

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.

1.2.1.- Desagregación de Procesos Críticos y Modelamiento de Riesgos

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 (el porcentaje mínimo se informará oportunamente por el Consejo de Auditoría Interna General de Gobierno) en una Matriz de Riesgos Estratégica. Esta técnica permite correlacionar la estructura desagregada de un proceso (subprocesos, etapas y actividades) con los objetivos operativos, el nivel de riesgo, el nivel de efectividad de los controles claves mitigantes y, finalmente, con el nivel de exposición al riesgo. En general, el Proceso de Gestión de Riesgos se inicia con los procesos más 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.
- Una vez identificados los procesos que desarrolla la organización gubernamental se debe realizar la desagregación de procesos y el modelamiento de los riesgos y los controles.

i.- Metodología

<u>Paso N° 1: Identificación y Priorización de Procesos Críticos en la Institución</u>

Para efectos de este documento, se entenderá como proceso un conjunto de actividades íntimamente interrelacionadas que existen para generar un bien o prestar un servicio, el cual

tiene uno o más clientes y proveedores, internos y/o externos a la organización en que opera. 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 siguientes criterios:

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.

Esquema de Relación y Priorización de Procesos Relevantes en la Institución en Relación a 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
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
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	-
……	.....	.....	.....	.....	.....	-
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

En el esquema anterior, se incluyen todos los procesos organizacionales y todos los objetivos estratégicos de la organización gubernamental. Se analiza cada proceso en relación con el nivel en que aporta al cumplimiento de cada objetivo, pudiendo ser de nivel Alto, Medio, Bajo o Nulo, de acuerdo con la escala anteriormente definida.

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 cada proceso crítico estará basada en la misma escala para el nivel en que afecta el cumplimiento del objetivo estratégico. Se deberá escoger para el análisis de procesos críticos, los que presenten un nivel de contribución promedio entre 2,0 y 3,0 puntos, es decir, se

seleccionarán los procesos claves que contribuyen desde un nivel importante a fundamental en el cumplimiento de todos los objetivos estratégicos institucionales o, dicho de otra forma, la relevancia de los procesos estará dada por el nivel de influencia o contribución que tiene cada proceso en el logro de los objetivos.

Ejemplo: Selección de procesos críticos en una organización que cuenta con tres objetivos estratégicos:

Misión Institucional : xxxxxxxx					
Objetivos / Procesos institucionales	**Objetivo Estratégico 1**	**Objetivo Estratégico 2**	**Objetivo Estratégico 3**	**Nivel de contribución promedio del proceso al cumplimiento de los objetivos**	**Proceso seleccionado (2,0 – 3,0)**
Abastecimiento	3	2	3	2,6	x
Financiero	2	1	0	1,0	
Crediticio	1	2	1	1,6	
Recursos Humanos	3	2	1	2,0	x
Comercialización	1	2	1	1,3	

Para este ejemplo, se debe realizar el análisis para los procesos críticos: Abastecimiento y Recursos Humanos.

En todo caso, independiente de la clasificación previamente explicada, la organización gubernamental debe considerar en el reporte al CAIGG, el porcentaje mínimo (valor porcentual mínimo) de procesos críticos que deben analizarse en la organización, que el CAIGG defina e informe a los servicios para que cumplan con esta materia.

Paso N° 2: Identificación de Subprocesos en los Procesos Críticos

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.

Paso N° 3: Identificación de Etapas en cada Subproceso

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.

Paso N° 4: Identificación de Objetivos Operativos

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.

Paso N° 5: Identificación de Riesgos Operativos Relevantes

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 o subproceso o 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.

Luego de la identificación del riesgo, se debe proceder a su medición (nivel de severidad del riesgo, de acuerdo con los criterios definidos en la escala presentada en el Anexo Nº 5 de este documento). Evaluando en términos de su probabilidad, como posibilidad de la 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 que se expone más adelante en este documento[12].

En forma complementaria debe calificarse la fuente y tipología de los riesgos de acuerdo con lo señalado al punto 1.2.4 de este documento.

Adicionalmente, para cada riesgo operativo relevante contenido en la Matriz de Riesgos Estratégica, se analizarán e identificarán si corresponde, señales de alerta relacionadas con los delitos de lavado de activos (LA), financiamiento del terrorismo (FT) o delitos funcionarios (DF), de acuerdo con lo señalado al punto 2.2.2.- Identificar Señales de Alerta para Delitos LA/FT/DF, asociadas a los riesgos.

Paso N° 6: Reconocimiento y Levantamiento de los Controles Claves

El próximo paso consiste en el reconocimiento y levantamiento de los controles que tiene la organización gubernamental y que se orientan a mitigar los riesgos operativos identificados. En

[12] Una guía básica para levantar información de los procesos y los elementos que deben considerarse, se contiene en el Anexo Nº 4 de este documento.

este punto, debe hacerse un análisis de los controles relevando sólo aquellos claves, cuyo objetivo es la mitigación de los riesgos. 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 5).

Luego, debe calcularse 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 5). Debe calcularse el riesgo ponderado por subproceso.

Paso N° 7: Formulación de la Matriz de Riesgos Estratégica

De la aplicación de este procedimiento se obtendrá como producto la "Matriz de Riesgos Estratégica" de la organización gubernamental al momento del análisis de los procesos críticos, la que contendrá los siguientes elementos:

- Procesos críticos de la organización (previamente priorizados).
- Identificación de subprocesos componentes de los procesos críticos de la organización y su ponderación.
- Identificación de etapas en cada subproceso (si corresponde).
- Identificación de los objetivos operativos por etapa o subproceso.
- Identificación de todos los riesgos operativos relevantes.
- Identificación de la fuente del riesgo y su tipología.
- Valor y clasificación de la severidad de los riesgos operativos.
- Identificación, valor y clasificación de la efectividad de los controles mitigantes asociados al riesgo operativo.
- Valor de la exposición al riesgo individual, por etapa, subproceso y proceso crítico.
- Valor de la exposición ponderada por subproceso.

Es importante destacar que la información recabada en la Matriz de Riesgos Estratégica de la organización gubernamental corresponde al momento en el cual se realiza este levantamiento de información, la que debe ser actualizada en forma periódica. Un ejemplo de levantamiento de proceso se establece en el Anexo Nº 6.

Acciones a Desarrollar Periódicamente

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

- Identificar los procesos que desempeña 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 (Ver punto 3.1.2).
- 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.
- 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° 7).
- Clasificar los riesgos por tipo y origen definidos en este Documento Técnico.
- Identificar señales de alerta de delitos LA/FT/DF asociados a los riesgos.
- Valuar los riesgos en relación con su probabilidad e impacto y a su nivel de severidad (criterios incluidos en el Anexo N° 5).
- 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?
- 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.

1.2.2.- Procesos Transversales en la Administración del Estado

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.

Acciones a Desarrollar Periódicamente

Para un adecuado Proceso de Gestión de Riesgos y el cumplimiento de la metodología contenida en este documento técnico, las organizaciones gubernamentales, deberán clasificar sus procesos en las categorías de procesos transversales que se señalan en el siguiente Cuadro Nº 1.

Cuadro Nº 1: 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.
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.

Procesos Transversales en la Administración del Estado	Descripción
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.
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.

Procesos Transversales en la Administración del Estado	Descripción
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 de Información	
Sistemas de información administrativos	Aquellos sistemas de información que entregan reportes y datos a los que puedan tener acceso 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.

Procesos Transversales en la Administración del Estado	Descripción
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.

Hay que tener presente que la clasificación que se hace en procesos de soporte, gerenciales, de negocio, entre otros, es solo genérica y referencial, ya que pueden existir organizaciones gubernamentales cuyos procesos de negocio correspondan a los que generalmente para las demás instituciones son de soporte, tales como; los procesos de contabilidad, de selección de recursos humanos, entre otros.

En el cuadro siguiente se entrega un ejemplo de dicha clasificación.

Cuadro Nº 2: 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	….	….	….	….

1.2.3.- Ponderación Estratégica por Subprocesos Componentes de Procesos Críticos

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 respectivo asesor del CAIGG.

Acciones a Desarrollar Periódicamente

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.

A continuación, en el Cuadro Nº 3 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 3: Ejemplo de Justificación de la Ponderación Estratégica de Subprocesos componentes de un Proceso Crítico

Proceso	Descripción	Subprocesos	Pond.[13]	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.
		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 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

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

Proceso	Descripción	Subprocesos	Pond.[13]	Justificación de la ponderación
				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%	…..

1.2.4.- Tipología de Riesgos

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 sirve para agrupar aquellos riesgos que tienen características y elementos comunes.

En relación con la fuente u origen de los riesgos, se puede señalar que existen riesgos de fuente externa y riesgos de fuente interna[14]. Los riesgos de fuente externa son aquellos que tienen su origen en situaciones que están fuera de la administración y control de la organización gubernamental, como los cambios políticos y sociales. Al contrario, son de fuente interna, los que se originan al interior de ella, como por ejemplo, los relacionados a las capacidades y competencias del personal y a la efectividad de los sistemas de información.

En el Cuadro Nº 6, 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 4: Ejemplos de Tipificación 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

[14] Cfr. COSO II. Gestión de Riesgos Corporativos.

Tipos de Riesgos	Elementos que los Caracteriza	Ejemplos de Riesgos Específicos
		- 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, demográfica, comportamientos sociales.	- Deficiente comportamiento de usuarios (bajo compromiso, bajo cumplimiento, etc.) - 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	- Falta de capacidad del personal - Personal sin capacitación

Tipos de Riesgos	Elementos que los Caracteriza	Ejemplos de Riesgos Específicos
	Gubernamental, desde su ingreso hasta su egreso del mismo.	- 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.)
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

Acciones a Desarrollar Periódicamente

Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, la organización gubernamental debe calificar los riesgos identificados de acuerdo con esta tipología de riesgos. La definición de estos criterios debe ser aplicada en la siguiente Fase de Identificación del Riesgo. 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 (Ver ejemplos en Anexo N° 8).

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.

1.3.- Criterio

Cada entidad debe precisar la cantidad y el tipo de riesgo que puede o no puede tomar (Apetito al 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.

Acciones a Desarrollar Periódicamente

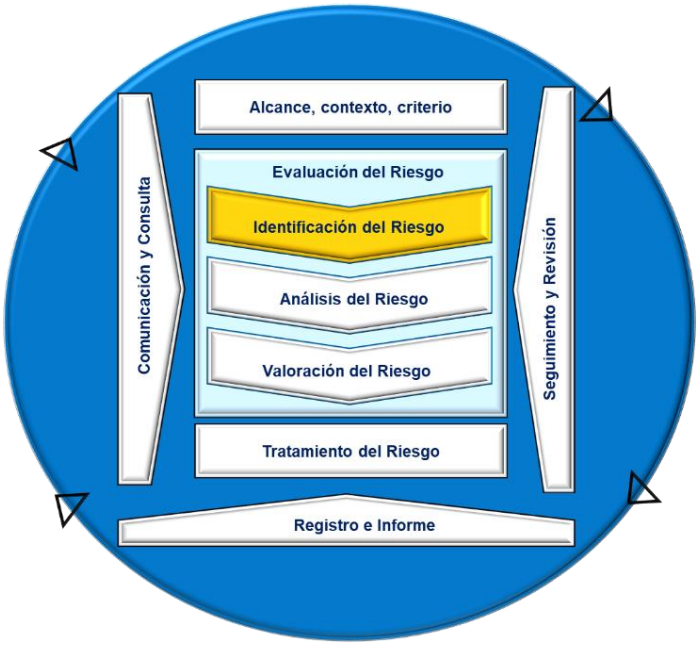
El Anexo N° 5 contiene una definición global y transversal para determinar los niveles de riesgos que se pueden tomar en las entidades públicas determinada por el CAIGG. Sin perjuicio de lo anterior, cada entidad debería evaluar en forma periódica cuán aplicable es la referida definición a su entidad, de acuerdo con sus actuales escenarios y la naturaleza y características organizacionales al momento de la evaluación.

En caso de que se requieran modificar los criterios presentados en el Anexo N° 5, cada entidad debe informar y presentar los respectivos antecedentes al CAIGG previamente a su aplicación, para una evaluación y aprobación técnica si correspondiese.

2.- FASE IDENTIFICACIÓN DEL RIESGO

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.

Gráfica N° 6: 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.[15] El riesgo es el efecto de la incertidumbre sobre el objetivo.[16]

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

2.1.- Identificación de Oportunidades

Un aspecto importante a 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 los mismos 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.

A continuación, en el Cuadro Nº 5 se entrega un ejemplo de identificación de oportunidades a través de eventos.

Cuadro Nº 5: 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	…..

Acciones a Desarrollar Periódicamente

[15] 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.
[16] NCh-ISO 31000:2018.

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.

2.2.- Identificación del Riesgo

La identificación de los eventos que puedan afectar negativamente el cumplimiento de los objetivos es fundamental en un Proceso de Gestión de Riesgos. En el Anexo Nº 7 se acompañan ejemplos de técnicas de identificación de eventos generadores de riesgos y oportunidades.

Acciones a Desarrollar Periódicamente

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.
- 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.

Por otra parte, 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 9). 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.

2.2.1.- Aplicación de la Tipología de Riesgos: Junto con identificar los riesgos, es importante clasificarlos según la tipología genérica formulada en la fase de establecimiento del contexto estratégico, considerando las categorías de riesgos a los que se pueden ver expuestas las entidades.

Acciones a Desarrollar Periódicamente

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 a continuación en el ejemplo del Cuadro Nº 6. 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.

Cuadro Nº 6: Ejemplo de Clasificación de Riesgos de Acuerdo a su Tipología

Proceso Transversal	Proceso	Subproceso	Pond.	Etapas	Objetivos	Riesgos específicos	Fuente de Riesgos	Tipo de riesgo	Prob.	Cons.	.....
Créditos – Recuperación de préstamos	Créditos de fomento a mujeres microempresarias	Recuperación del crédito	25%	Cobranza	Recuperar oportunamente los créditos	Falta de acciones oportunas de cobranza	**Interna**	**Procesos**	3	3	…
						Insolvencia de los deudores	**Externa**	**Económico**	2	4	…
					Contar con garantías de los créditos	Falta de garantías	**Interna**	**Procesos**	1	4	…
				Ingreso fondos recuperados	Ingresar los fondos recuperados en forma oportuna y completa	Ingreso inoportuno o incompleto de pagos	**Interna**	**Personas**	4	3	…
						Errores en la digitación de los montos	**Interna**	**Personas**	3	4	…
						Problemas en la transformación de la información del sistema de la Organización Gubernamental al SIGFE	**Interna**	**Tecnológico**	2	4	…
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…

Se deberá revisar la clasificación de los riesgos realizada de acuerdo con la tipología desplegada en el Cuadro Nº 6 anterior, prestando especial atención a dos puntos específicos:

a) Los riesgos deben ser clasificados según su fuente como externos o internos. Para ello, debe estarse principalmente al origen del riesgo, esto es a su causa. Por ejemplo, un riesgo relacionado con la mala calidad de los datos e información de la organización gubernamental, es un riesgo de origen interno, independientemente que la administración del sistema de información se haya externalizado, ya que el riesgo parte de una debilidad interna. En cualquier caso, debe clasificarse sólo en una fuente, no siendo válido un riesgo interno/externo, debiendo optarse por aquella fuente que tenga mayor importancia en el origen del riesgo.
b) Los riesgos deben ser clasificados solo en una de las tipologías definidas en este documento técnico. Para ello, debe considerarse principalmente la causa de este. Por ejemplo, si se identifica un riesgo de corrupción o de falta de probidad en el personal, nos encontramos con un riesgo que se clasifica en la tipología “personas” aun cuando sus consecuencias afectan también a la imagen de la organización gubernamental.

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

Entre otras recomendaciones, al redactar los riesgos identificados se sugiere considerar siempre la causa y el efecto que se genera en el ámbito donde están siendo analizados. Por ejemplo, El déficit de competencias del personal genera errores y deficiencias en el proceso.

2.2.2.- Identificar Señales de Alerta para Delitos LA/FT/DF, asociadas a los riesgos

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.

a) Para cada riesgo identificado en la Matriz de Riesgos Estratégica, se deberá asociar, si corresponde, señales de alerta para delitos LA/FT/DF[17]. 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:

- 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).

b) 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

[17] Las señales de 3alerta 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° 13.

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.

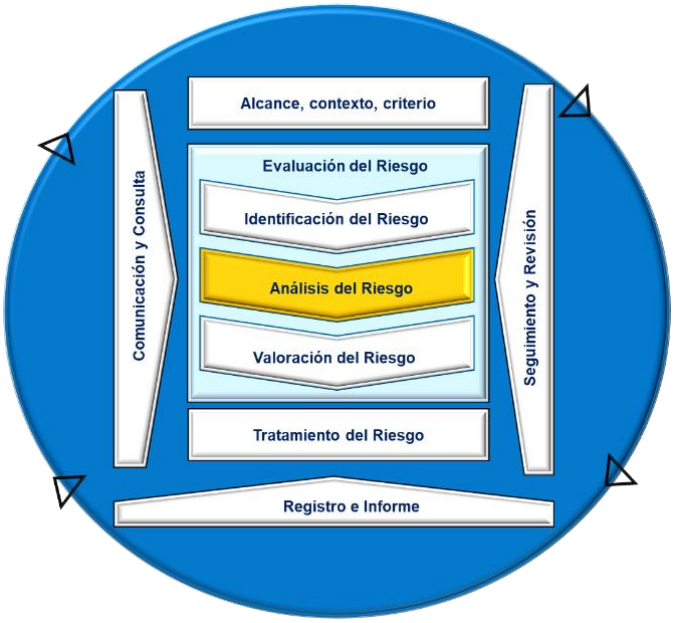
Para levantar la información y comunicar del resultado del análisis de los requerimientos de la letra b) al CAIGG, se debe cumplir con lo dispuesto en el Anexo N° 14. Señales de Alerta LA/FT/DF No Asociadas con los Riesgos Incluidos en la Matriz de Riesgos Estratégica.

3.- FASE ANÁLISIS DEL RIESGO

3.1.- Análisis General de Riesgos

Las Organizaciones Gubernamentales después de desarrollar la identificación de riesgos operativos, deben analizarlos, examinando los riesgos en relación con su probabilidad y consecuencias. A su vez, los controles deben ser analizados en términos de efectividad, para finalmente identificar el nivel de exposición al riesgo por proceso, subproceso, etapa y riesgo específico.

Gráfica N° 7: Fase Análisis del Riesgo



Fuente: NCh-ISO 31000:2018 – INN

Existen dos elementos que deben considerarse en esta fase:

3.1.1.- Análisis de los Riesgos: 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.

Acciones a Desarrollar Periódicamente

Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, la organización gubernamental debe analizar los riesgos y oportunidades, poniendo especial énfasis en los siguientes puntos:

- Analizar y/o actualizar los riesgos y su calificación de probabilidad e impacto, de acuerdo con las últimas auditorías, los antecedentes históricos que se tengan y a los cambios que hayan afectado a la institución (modificaciones presupuestarias, nuevos objetivos, eliminación de programas, cambios en las políticas gubernamentales, modificaciones en la orientación y lineamientos de la dirección, entre otras situaciones).
- Analizar y/o actualizar los riesgos, con especial énfasis en los riesgos asociados con aspectos estratégicos y financieros, considerando los recursos involucrados en los procesos y subprocesos y el uso de estos.
- Considerar la retroalimentación de la unidad de auditoría interna, ya sea a través de los trabajos de aseguramiento, consultoría y seguimiento del Proceso de Gestión de Riesgos, así como las auditorías a los diversos procesos de la organización gubernamental.
- Analizar y/o actualizar los riesgos de Gobierno Electrónico, analizando qué procesos han sido mejorados con TIC y cómo ello influye en su desarrollo, teniendo en consideración que muchas veces el mejoramiento de las TIC se realiza en etapas o actividades del proceso, pero su influencia e impacto irradia la totalidad de este. Ver Anexo N° 8.
- Analizar y/o actualizar los riesgos de la organización gubernamental, considerando los nuevos enfoques y lineamientos del Gobierno, así como los cambios que experimentan los riesgos identificados en años anteriores.
- 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.
- Relacionar adecuadamente los riesgos con el objetivo de la etapa. Esto implica que la concreción de un riesgo debe afectar el cumplimiento o logro de la etapa en forma directa, de tal manera que los riesgos identificados impidan o dificulten el resultado esperado por la organización gubernamental al desarrollar esa etapa.
- Analizar y/o actualizar la descripción de los controles de acuerdo con los resultados de las auditorías realizadas, los antecedentes históricos que se tengan y a los cambios que hayan afectado a la organización gubernamental (modificaciones presupuestarias, nuevos objetivos, eliminación de programas, entre otras situaciones); determinando si estos controles están documentados y si existe una adecuada segregación de funciones. Ver Anexo Nº 9.
- 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**. 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).

- Ajustar las exposiciones al riesgo de acuerdo con las actualizaciones realizadas a los riesgos y controles.

3.1.2.- 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[18] por el porcentaje de ponderación estratégica que a cada uno de ellos le fue asignado, de la forma que se explica en el cuadro a continuación:

Cuadro Nº 7: Ejemplo de Ponderación Estratégica por Subprocesos

Proceso Transversal	Proceso	Subproceso	Pon[19]	Etapas	...	Nivel de Exposición al Riesgo				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 7, 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.

Acciones a Desarrollar Periódicamente

Para la adecuada implantación, mantención y actualización del Proceso de Gestión de Riesgos, la organización gubernamental debe definir las ponderaciones o revisarlas y mejorarlas, de acuerdo con lo señalado en el punto 1.2.3 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.

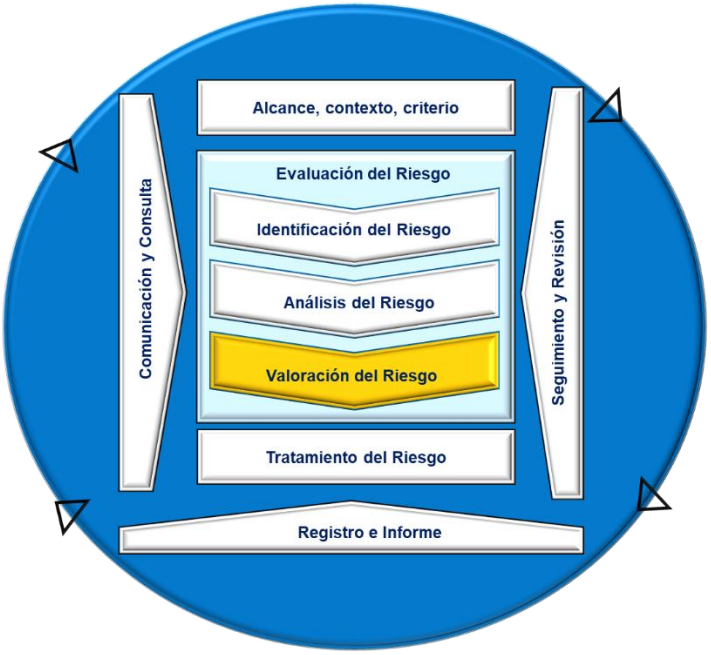
[18] Nivel determinado en base a las escalas definidas en el Anexo Nº 5 de este documento.

4- 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.

Gráfica N°8: Fase Valoración del Riesgo



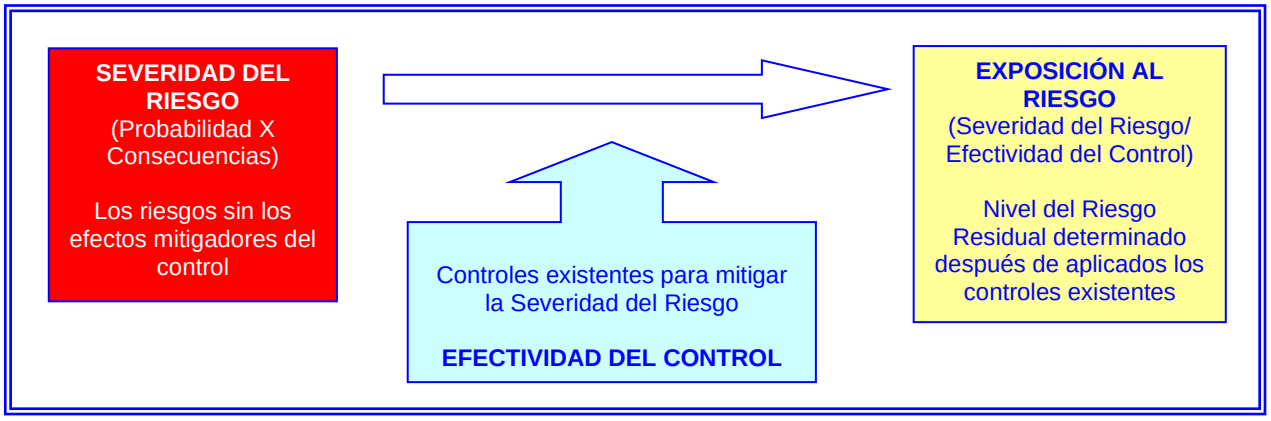
Fuente: NCh-ISO 31000:2018 – INN

4.1.- 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 el Cuadro Nº 8 que se presenta a continuación, se muestra la relación entre los distintos componentes del análisis de riesgos.

Cuadro Nº 8: Relación entre Severidad del Riesgo y Exposición al Riesgo



4.2.- 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:

a.- Ranking de Procesos por Nivel de Exposición al Riesgo

En el Cuadro Nº 9 se presenta el esquema del análisis a realizar para un proceso crítico que fue desagregado hasta el nivel de riesgo operativo.

Cuadro Nº 9: Ejemplo de Ranking de Procesos por Nivel de Exposición al Riesgo

Procesos	Nivel de Exposición al Riesgo	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.

b.- Ranking de Subprocesos por Nivel de Exposición al Riesgo 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:

Cuadro Nº 10: 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°**	…	…	…	…
	….	….	**….**	…	…	…	…
2° Capacitación	Subproceso 2	1,7	**1°**	Etapa 2	…	…	…
	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.

Acciones a Desarrollar Periódicamente

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 Nº 9 y N° 10, respectivamente, como apoyo para el señalado ranking.

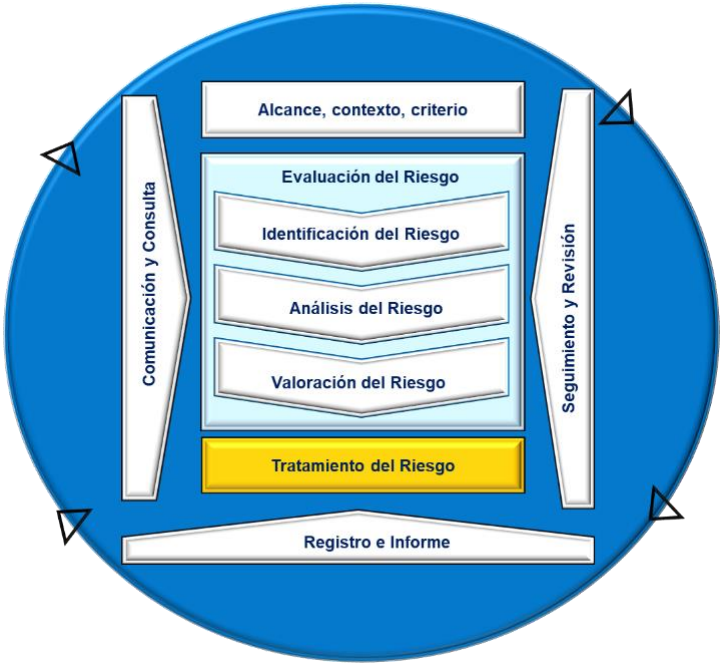
Es importante que, en base la información proporcionada por los Ranking de Procesos y Subprocesos (incluyendo el Ranking de Etapas), la organización gubernamental determine qué etapas, subprocesos y procesos serán abordados con acciones para tratar los riesgos específicos. Dicha determinación debe fundamentarse 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.

5.- FASE TRATAMIENTO DE RIESGOS

La Fase Tratamiento de Riesgos, 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.

Gráfica N° 9: Fase Tratamiento del Riesgo



Fuente: NCh-ISO 31000:2018 – INN

5.1.- 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.

5.2.- 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, 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 11: 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.

5.3.- 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 12 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 12: 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.

5.4.- 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.

Acciones a Desarrollar Periódicamente

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 sus riesgos (a nivel de proceso) dentro de los límites tolerables.
- Las estrategias escogidas deberían ser: reducir, aceptar, compartir o evitar, 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 10.

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 15 siguiente:

Cuadro Nº 13: 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 15	
N° Descriptor	**Significado**
(1)	Proceso genérico, transversal o megaproceso al cual corresponde el proceso priorizado, de acuerdo a la clasificación del documento (Cuadro Nº 3).
(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.
(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 6.
(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.

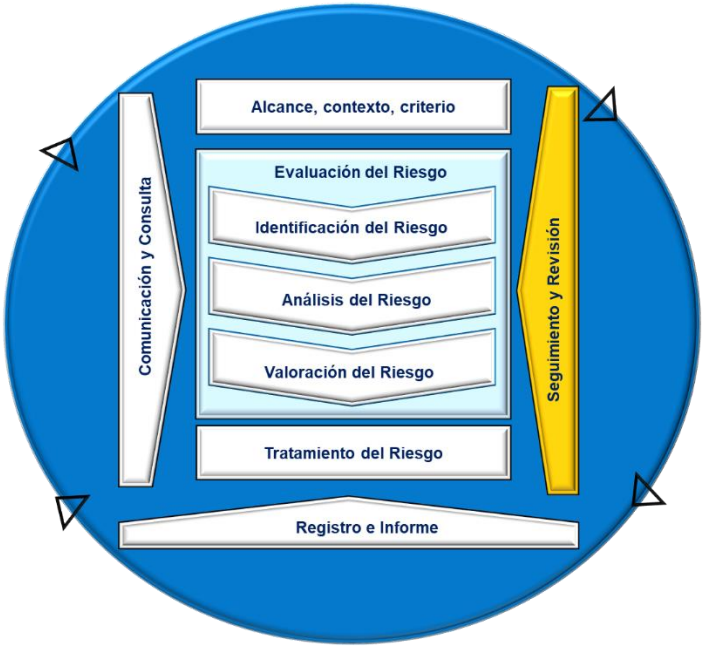
6.- FASE SEGUIMIENTO Y REVISIÓN

En esta fase es necesario nombrar responsables de monitorear 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.

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.

También es conveniente, internalizar en la cultura organizacional la implantación y utilización de modelos de autoevaluación de riesgos.

Gráfica N° 10: Fase Seguimiento y Revisión



Fuente: NCh-ISO 31000:2018 – INN

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.

Acciones a Desarrollar Periódicamente

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° 14.

Cuadro Nº 14: 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 16 (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.

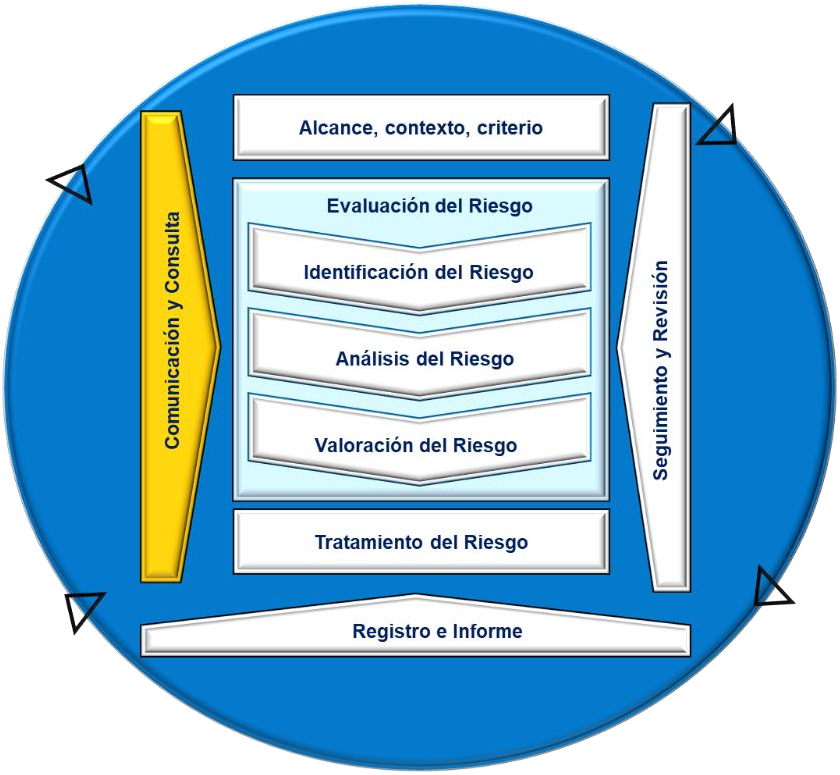
7.- FASE COMUNICACIÓN Y CONSULTA

Sin perjuicio que para efectos metodológicos esta fase se explicará a continuación, en general es una de las primeras que se debería desarrollar en la implantación de un Proceso de Gestión de Riesgos. En ella se desarrollarán planes de comunicación y consulta, para informar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos. La información debe ser identificada, capturada y comunicada de manera que todos puedan cumplir con sus roles y deberes y para asegurarse que aquellos responsables de la implementación del Proceso y las partes interesadas comprenden las bases que han servido para tomar decisiones y las razones por las que son necesarias determinadas acciones.

La idea es que los interesados internos (la organización gubernamental) y los externos que corresponda (autoridades, CAIGG, etc.) estén informados de la marcha del Proceso de Gestión de Riesgos y de qué manera se van implementando las medidas para el tratamiento de riesgos. Para esto es importante que los informes y sistemas de información ofrezcan suficientes datos relevantes para posibilitar una comunicación y control eficaz.

En consideración a que el objetivo fundamental de esta fase es obtener y entregar información confiable en todas las fases del Proceso de Gestión de Riesgos, en primer lugar, se debería elaborar o actualizar “Planes de Comunicación y Consulta”, adaptados a la realidad de la organización, considerando como mínimo los siguientes componentes y antecedentes:

Gráfica N° 11: Fase Comunicación y Consulta



Fuente: NCh-ISO 31000:2018 – INN

7.1.- 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 15.

Sin perjuicio de la periodicidad en que el Jefe de Servicio y el Consejo de Auditoría 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 15: 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.
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			
....	....	....	....

7.2.- 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.

Acciones a Desarrollar Periódicamente

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[20], 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 15.

  - **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 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 a 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 Consejo de Auditoría 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.

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

- 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 Consejo de Auditoría cuando éste lo solicite.

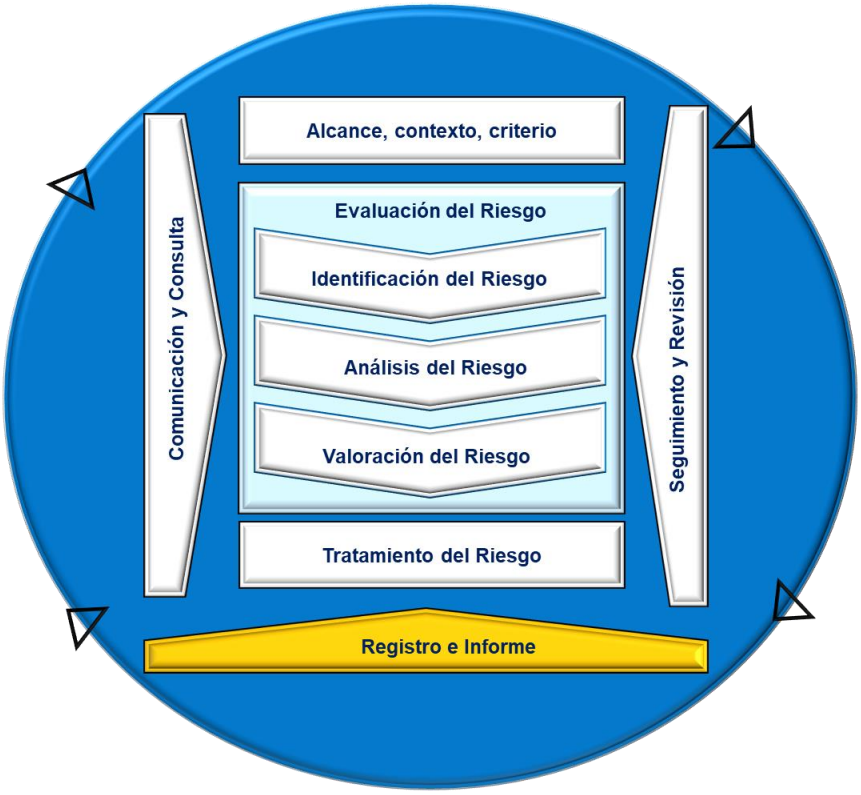
8.- FASE REGISTRO E INFORME

De acuerdo con la NCh-ISO 31000:2018, las actividades de gestión del riesgo deberían ser trazables. En el Proceso de Gestión del Riesgo los registros proporcionan la base para la mejora de los métodos y de las herramientas, así como del proceso en su conjunto.

Las decisiones relativas a la creación de registros deberían tener en cuenta los siguientes puntos:

- Las necesidades de la organización en materia de aprendizaje continuo.
- Los beneficios de reutilizar la información para fines de mejora de la gestión.
- Los costos y los esfuerzos que involucran la creación y la mantención de los registros.
- Las necesidades legales, reglamentarias y operacionales para efectuar los registros.
- El método de acceso, la facilidad de recuperación y los medios de almacenaje.
- El período de conservación.
- El carácter sensible de la información.

Gráfica N° 12: Fase Registro e Informe



Fuente: NCh-ISO 31000:2018 – INN

Acciones a Desarrollar Periódicamente

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.

C.- REPORTES DEL PROCESO DE GESTIÓN DE RIESGOS AL CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

El Consejo de Auditoría Interna General de Gobierno 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.

VII.- BIBLIOGRAFÍA

- Consejo de Auditoría Interna General de Gobierno, Documento Técnico Nº 41 – Gestión de Riesgos, 2009.
- Consejo de Auditoría Interna General de Gobierno, Documento Técnico Nº 45 – Gestión de Riesgos, 2010.
- Consejo de Auditoría Interna General de Gobierno, Documento Técnico Nº 59 – Gestión de Riesgos, 2014.
- 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).
- 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
- Instituto de Auditores Internos (IIA), Practice Guide: Assessing the Adequacy of Risk Management Using ISO 31000, 2010.
- Instituto de Auditores Internos (IIA), International Professional Practices Framework (IPPF), EEUU, 2011.
- International Organization for Standardization, ISO 31000:2018 - Directrices para la Gestión de Riesgos, 2018.
- International Organization for Standardization, Internacional ISO/TR 31004:2013. Risk management - Guidance for the implementation of ISO 31000, 2013.
- Instituto Nacional de Normalización, Norma NCH-ISO 31000:2018 - Directrices para la Gestión de Riesgos, 2018.
- Instituto Nacional de Normalización, Norma NCH-ISO Guía 73:2012 - Gestión del Riesgo – Vocabulario, 2012.
- Instituto Nacional de Normalización, Norma NCH-ISO 31010:2020 - Gestión del Riesgo - Técnicas de Evaluación del Riesgo, 2020.
- Instituto Nacional de Normalización, Norma NCH-ISO 31004:2014 Gestión del Riesgo – Orientación para la implementación de ISO 31000, 2014
- Instituto de Auditores Internos de España, Definición e Implantación de Apetito de Riesgo, 2013.
- Oficio Circular N° 20/2015 del Ministerio de Hacienda. Orientaciones generales para el Sector Público en relación con el inciso sexto del artículo 3° de la ley N° 19.913.
- Organización para la Cooperación y el Desarrollo Económicos - Principios de Gobierno Corporativo de la OCDE, 2004.
- Open Compliance & Ethics Group, OCEG Red Book GRC Capability Model 3.0.
- Sponsoring Organizations of the Treadway Commission (COSO), Gestión del Riesgo Empresarial, Marco Integrado – Integrando Estrategia y Desarrollo, 2017.
- Sponsoring Organizations of the Treadway Commission (COSO), Internal Control - Integrated Framework, 2013.

ANEXO Nº 1

EJEMPLO 1: MODELO DE POLÍTICA DE GESTIÓN DE RIESGOS

La gestión de riesgos proporciona a nuestro (Servicio, Empresa, Entidad, etc.,) la capacidad para identificar, evaluar y gestionar todo el espectro de riesgos que pueden afectar al Servicio y posibilitar que todo el personal mejore su comprensión del riesgo, lo que permite obtener:

- Aceptación responsable del riesgo.
- Apoyo a la dirección.
- Mejoras en los resultados.
- Responsabilidad reforzada.
- Liderazgo superior.

La presente política, que asigna especial importancia a la reducción de los riesgos, obedece al propósito de mejorar la gestión institucional, a fin de contribuir al cumplimiento de sus objetivos estratégicos y con ello, al logro de su misión.

Como elementos importantes en la Gestión de Riesgos se considerarán:

- La utilización de la norma chilena ISO NCh-ISO 31000:2018 como marco principal para la gestión de riesgos integral en la organización.
- La integridad y consistencia de los procedimientos administrativos y procesos asociados.
- La calidad de la gestión de los recursos humanos a través, fundamentalmente, de sus habilidades, perfiles y entrenamiento.
- La infraestructura.
- La pertinencia, oportunidad y seguridad de la información.

Prevalecerá el enfoque PREVENTIVO y PROACTIVO.

La metodología para determinar el nivel de Apetito de Riesgo es una ponderación global del nivel de riesgo que la máxima autoridad del Ministerio está dispuesta a aceptar para el logro de los objetivos institucionales, de acuerdo con lo establecido en el Documento Técnico N° 70 del Consejo de Auditoría Interna General de Gobierno (CAIGG), en su última versión o el que lo reemplace.

El proceso de Gestión de Riesgos dará cumplimiento a los siguientes aspectos:

- La existencia de un ambiente controlado de gestión de riesgos que, definido por la Dirección, establezca estrategias corporativas y una estructura de supervisión adecuada que garantice su operatividad.
- La definición y documentación de la exposición al riesgo a lo largo de los procesos y lineamientos, de acuerdo con los criterios de las Normas de Calidad.
- La cuantificación del impacto y probabilidad de ocurrencia para cada uno de los riesgos identificados.
- Evaluación y seguimiento permanente de eventos que generen perjuicios a la entidad.

Nuestra Misión consiste en entregar apoyo a la mujer microempresaria, entregándole soporte a la mujer emprendedora con instrumentos de fomento, créditos flexibles y capacitación para los

negocios. Lo anterior implica importantes riesgos, pero también oportunidades. Por una parte, la mujer ha tomado un papel de importancia en la sociedad y ha escalado posiciones de poder y empresariales de relevancia. Además, la mujer en general es puntual en el pago de sus obligaciones y en el cumplimiento de sus compromisos. Sin embargo, también surgen riesgos relacionados con la vulnerabilidad del sector al que está orientada la organización, ya que se trata de mujeres de bajos ingresos y nivel cultural. Además, la expansión del comercio electrónico obliga a capacitar a nuestras usuarias en el uso y manejo de las tecnologías que les permitan insertarse en el mundo de los negocios.

Consideramos que enfrentamos un gran desafío y estamos conscientes que debemos capacitar a nuestras usuarias para que enfrenten el complejo mundo de los negocios, esto implicará una gran inversión en recursos humanos y tecnológicos y una constante medición de nuestros resultados, para determinar nuestros avances y retrocesos.

Para el Proceso de Gestión de Riesgos, se incorporarán todos los procesos que desarrolla la organización, tanto aquellos de negocio, esto es, los que se relacionan directamente con el cumplimiento de su Misión, como los de soporte.

En el marco del proceso de Gestión de Riesgos, la Dirección Ejecutiva utilizará la metodología del Consejo de Auditoría esto es, se levantarán estos procesos, desagregándose por subproceso, etapas, actividades y riesgos y priorizará los procesos y subprocesos en función de la importancia relativa de cada uno de ellos en el cumplimiento de la misión institucional y objetivos estratégicos, para luego ser administrados, utilizando alguna de las siguientes estrategias genéricas, que no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias., adecuadas a la realidad de la organización gubernamental:

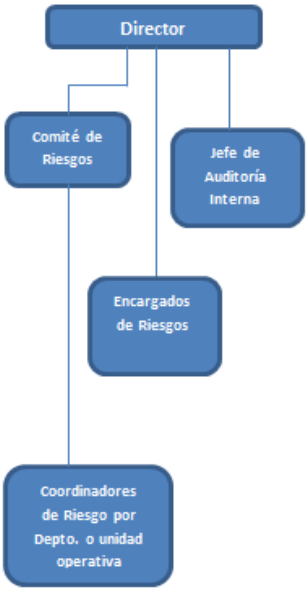
- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que causa el riesgo.
- Aceptar o aumentar el riesgo a fin de perseguir una oportunidad.
- Eliminar la fuente del riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo con otras partes (incluyendo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

Cualquiera estrategia que se elija, debe estar adecuadamente justificada y estar aprobada por la dirección.

La Dirección de la organización gubernamental se compromete periódicamente a realizar una revisión de la política de riesgos aquí establecida.

ANEXO Nº 2

EJEMPLO 1: MODELO DE DEFINICIÓN DE ROLES Y RESPONSABILIDADES

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: MODELO DE DEFINICIÓN DE ROLES Y RESPONSABILIDADES

Roles Claves	**Responsables**	**Tareas y Actividades**
SUPERVISOR Y COORDINACION DE DECISIONES	Jefe de Servicio	Definir el Apetito al Riesgo para la institución. 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. Remitir por oficio al CAIGG los reportes del proceso de gestión de riesgos en el Ministerio según las instrucciones que correspondan.
	Comité de Riesgos	Proponer alternativas para la definición del Apetito al 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. 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. 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	Unidad 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.

ANEXO Nº 3

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[21] 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[22] 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.

[21] 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 – Instituto de Auditores Internos - THEIIA.
[22] 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 4

GUÍA BÁSICA PARA EL LEVANTAMIENTO DE INFORMACIÓN DE LOS PROCESOS Y MODELAMIENTO DE RIESGOS[23]

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):

- El tipo de proceso; estratégico o de soporte.

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

- 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.

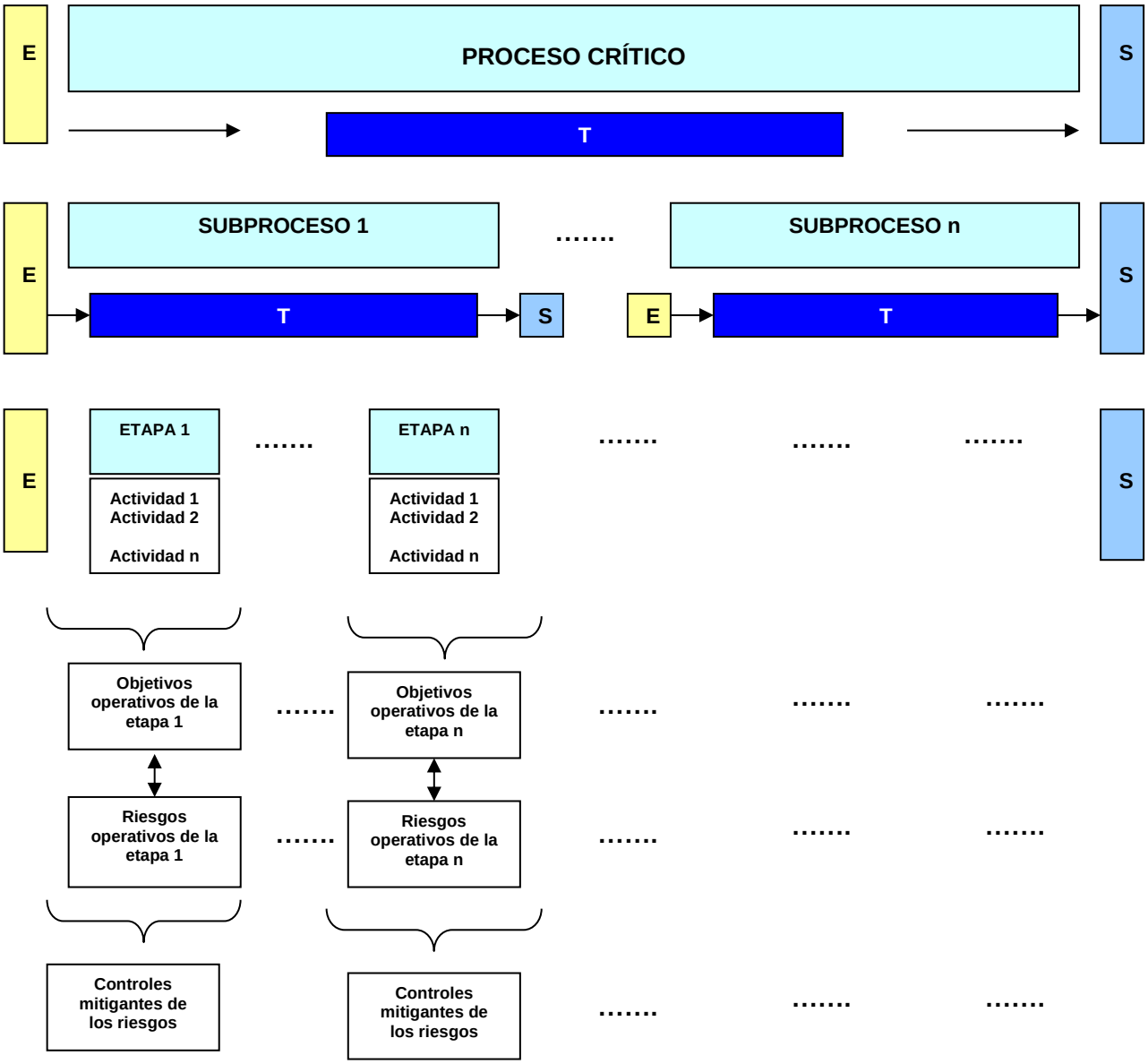
Posteriormente, se deben identificar todos los eventos que podrían afectar negativamente la consecución del objetivo operativo de cada etapa. Este aspecto es recomendable analizarlo desde el punto de vista de cómo afectan a dicho objetivo, las amenazas, errores o deficiencias de las entradas al subproceso 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 5

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 las siguientes relaciones:

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 4: 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 5: 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 6: 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 7: 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	SEMI INFORMAT	REGULAR	2
CUMPLIMIENTO ADECUADO	OCASIONAL	CORRECTIVO	SEMI INFORMAT		
CUMPLIMIENTO ADECUADO	OCASIONAL	DETECTIVO	SEMI INFORMAT	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 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 9.

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 8: 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 9.

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.

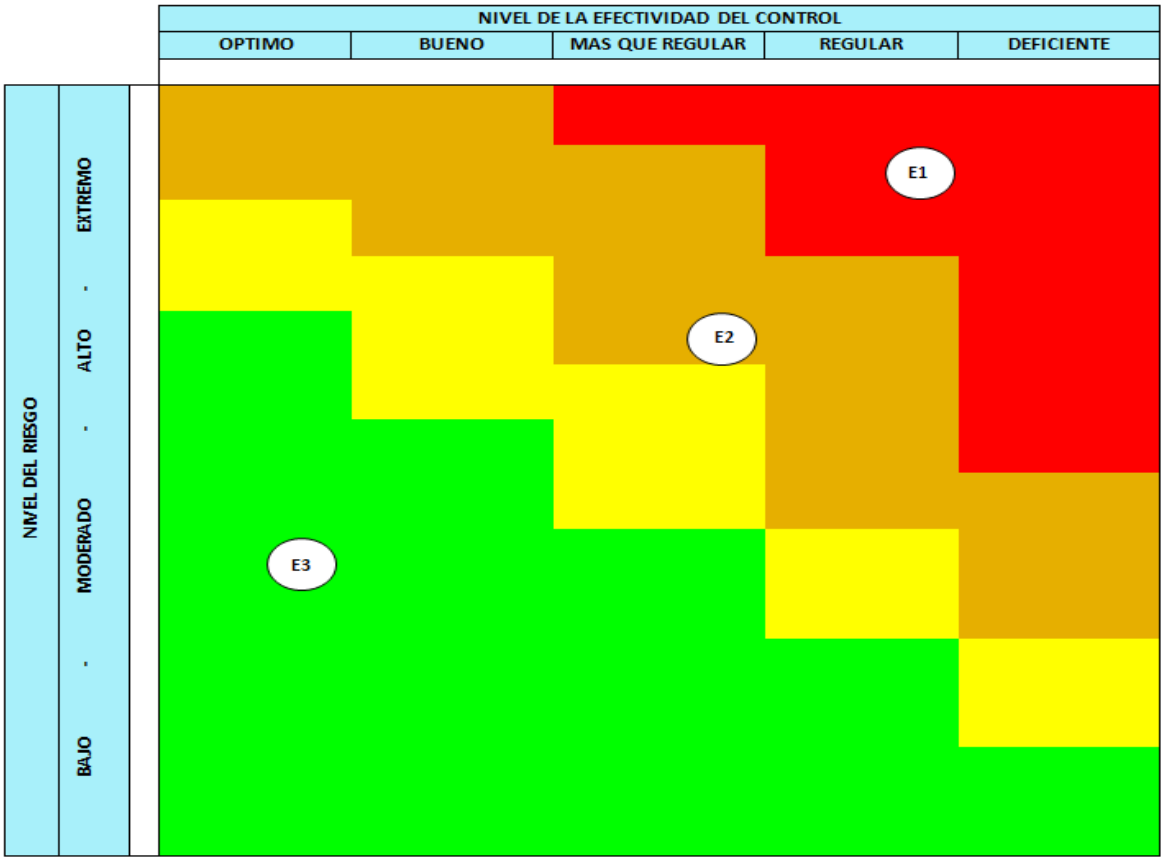
Por otra parte, los niveles de exposición al riesgo más bajos están conformados por las combinaciones entre los niveles de riesgos menos severas y los niveles de eficiencia del control más altos, o por las combinaciones entre riesgos con severidades Bajas y controles con niveles de efectividad Deficiente 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 9 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 9: Relaciones Entre Severidad del Riesgo y Efectividad del Control que Determinan la Escala del Nivel de Exposición al Riesgo



ANEXO Nº 6

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
Etapa Confección y publicación de bases.		1.- Se realiza la definición de especificaciones técnicas (características, plazos, volúmenes, calidades, etc.).		Encargado de especificaciones técnicas de compras

Etapas	Objetivo operativo de la etapa	Actividades de la etapa		Responsables
		De gestión	De control	
	Establecer formalmente bases administrativas y técnicas adecuadas a la especificación técnica de lo requerido y que respeten la transparencia e igualdad de los oferentes.		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
			7.- Entrega de reportes del sistema al comité de compras.	Encargado del sistema de compras y supervisor

Etapas	Objetivo operativo de la etapa	Actividades de la etapa		Responsables
		De gestión	De control	
		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…	…	…	…
	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.
			La apertura no se realiza a través del sistema y no se cumple el procedimiento aprobado.

Etapa	Objetivo operativo de la etapa	Actividades de la etapa	Riesgos asociados a la realización de las actividades
Etapa Selección		2.- Apertura de acuerdo a la normativa de compras a través del sistema de Chilecompras.	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 lo 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 respecto de funcionarios de la organización gubernamental y cumplan obligaciones laborales.	Inexistencia de antecedentes para realizar la verificación
			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

ANEXO Nº 7

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 SI…?" (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.

Para mayor información sobre esta materia se recomienda leer la norma NCh-ISO 31010:2013, emitida por el Instituto Nacional de Normalización, INN (www.inn.cl) y el Documento Técnico N° 75: Técnicas y Herramientas para el Control de Procesos y la Gestión de la Calidad, para su uso en la Auditoría Interna y en la Gestión de Riesgos, disponible en http://www.auditoriainternadegobierno.cl/.

ANEXO Nº 8

EJEMPLOS DE RIESGOS Y CONTROLES RELACIONADOS CON EL GOBIERNO ELECTRÓNICO

Para identificar adecuadamente los riesgos que pueden afectar los procesos mejorados con Tecnología de la Información, es necesario tener presentes las siguientes consideraciones generales:

1) Fragilidad de los Sistemas de Información

Al identificar los riesgos en las etapas o actividades de los procesos desagregados, hay que tener presente que los sistemas de información informatizados son vulnerables a una diversidad de amenazas y atentados por parte de:

- Personas tanto internas como externas de la organización.
- Desastres naturales.
- Servicios, suministros y trabajos no confiables e imperfectos.
- Incompetencia y las deficiencias cotidianas.
- Abuso en el manejo de los sistemas informáticos.
- Desastres a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

2) Inseguridad de la Información

Otro punto importante para considerar, al identificar los riesgos en los procesos desagregados, es que la información contenida en soporte electrónico, en términos generales puede presentar las siguientes situaciones de riesgo:

- **Riesgos de Integridad**: Este riesgo abarca todos aquellos relacionados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos existen en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en la Interfase del usuario, procesamiento de errores y administración de cambios.
- **Riesgos de Usabilidad**: Se refiere a los riesgos relacionados al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).
- **Riesgos de Acceso**: Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Abarcan los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información.
- **Riesgos de Recuperabilidad**: Relacionados con las deficiencias en las técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas y los backups y planes de contingencia que controlan desastres en el procesamiento de la información, entre otros.

- **Riesgos en la Infraestructura**: Estos riesgos se refieren a que en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.
- **Riesgos de Seguridad General**: Referidos a los Riesgos de choque de eléctrico, riesgos de incendio, de niveles inadecuados de energía eléctrica, de radiaciones, mecánicos, etc.

3) Riesgos Relacionados con los Documentos Electrónicos

Por último, es importante destacar que en las organizaciones, cuyas actividades constan en documentos electrónicos y éstos son el respaldo de las transacciones y operaciones que desarrolla la institución, pueden presentarse algunos riesgos relacionados con éstos documentos, que deben ser considerados:

- **Riesgos de Autorización**: Relacionados al hecho que la información electrónica haya sido creada, procesada, grabada, corregida, enviada, archivada, accesada y destruida sólo por personas autorizadas y responsables.
- **Riesgo de Autenticación**: Referidos a los medios para verificar la identidad declarada de un usuario y la autorización o denegación del acceso al sistema, y la forma como la autenticación permite a cada lado de la comunicación asegurarse de que el otro es quien dice ser.
- **Riesgo de Integridad**: Son aquellos que se relacionan con la exactitud, completitud y oportunidad de los datos, referidos a la modificación de la información, por error o intencionalmente.
- **Riesgos de Confidencialidad**: Referidos la capacidad de mantener un documento electrónico protegido y accesible para su divulgación o revelación sólo a una lista determinada de personas autorizadas y responsables.
- **Riesgos de No Repudio**: Relativo a la capacidad del sistema de permitir a cada lado de la comunicación, probar fehacientemente que el otro lado ha participado; de tal forma que el origen no pueda negar haberlo enviado y el destino no pueda negar haberlo recibido.
- **Riesgos de Accesibilidad**: Relativo a la mantención de datos disponibles permanentemente para cumplir con su misión y con sus obligaciones legales, tributarias y para propósitos de auditoría.

Para identificar los controles, se debe tener presente que en el caso de sistemas de información, es posible encontrar controles generales, que pueden intervenir en forma habitual a los riesgos relevados en los procesos, como los son las políticas y procedimientos aprobados y difundidos acerca de la seguridad sobre accesos digitales y físicos, la segregación de funciones incompatibles y accesos de control, la retención, archivo o almacenamiento, accesibilidad, distribución y destrucción de documentos electrónicos y otros datos, la administración de pistas o rastros de auditoría (*Audit Trail*). También pueden considerarse como controles generales los contratos con proveedores de servicios de tecnologías de información, la capacitación y generación de competencias, las instrucciones sobre correo electrónico seguro, el monitoreo del cumplimiento de los procedimientos establecidos y la tecnología basada en encriptación de datos, firmas electrónicas y certificados digitales.

Por otra parte, es necesario considerar que pueden existir controles específicos para los riesgos específicos, a saber:

- **Controles para Riesgos de Autenticación**: *Smart card* o *tokens*, *Password,* Biometría, PKI Infraestructura de clave pública, certificados digitales, *Firewalls*, etc.
- **Controles para Riesgos de Integridad**: Control de acceso a aplicaciones, funciones automáticas que permitan segregación de funciones, validación de datos, reportes de excepciones, controles de secuencia numérica y de coincidencia, control de rastros de correcciones, firma electrónica, *firewalls* entre otros.
- **Controles para Riesgos de No Repudio**: Técnicas criptográficas, certificados digitales, firma electrónica avanzada, *time stamping*, entre otros.
- **Controles para Riesgos de Autorización**: Controles de acceso, definición de perfiles de usuario en redes, aplicaciones y sistemas; firma electrónica, certificados digitales, etc.
- **Controles para Riesgos de Disponibilidad**: Controles asociados a la adquisición, desarrollo y mantenimiento de sistemas, mecanismos de recuperación de pérdida de datos, planes de contingencia, políticas de respaldo periódico de la información, y otros.
- **Controles para Riesgos de Confiabilidad**: Cifrado o encriptación, controles de acceso lógico y físicos a los sistemas y servidores, procedimientos de manipulación de copiado, almacenamiento, transmisión y destrucción, documentos reservados con niveles de acceso determinados, protocolos de seguridad sobre Internet (SSL), *firewalls*, entre otros.

ANEXO Nº 9

CONCEPTOS GENERALES SOBRE REQUISITOS BÁSICOS DE CONTROL ADECUADO CONSIDERADOS EN EL MODELO

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[24].

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[25].

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[26].

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.

[24] COSO I
[25] COSO I
[26] 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.

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[27].

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 beneficios se modifica, surgen exigencias nuevas, aparecen tecnología 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.

[27] Normas Internacionales para el Ejercicio de la Profesión de Auditoría Interna - IIA

- **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 a 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[28].

El Marco COSO versión 1992 fue mejorado en el 2013[29] 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.

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.

[28] COSO I
[29] 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.

- 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

1. La organización demuestra compromiso con la integridad y los valores éticos.
2. La máxima autoridad[30] demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.
3. 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.
4. La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en alineación con los objetivos de la organización
5. La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.

Evaluación de Riesgos

6. La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.
7. 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.

[30] En las organizaciones del Sector Público el equivalente al Consejo es la Máxima Autoridad o Jefe de Servicio.

8. La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.
9. La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.

Actividades de Control

10. 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.
11. La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.
12. 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

13. La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.
14. La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.
15. La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.

Actividades de Supervisión

16. 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.
17. 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**).

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	Qué: Registro automatizado. Cómo: El sistema de control biométrico registra las horas trabajadas y calcula aquellas que exceden de las 44 horas ordinarias. Cuándo: Diariamente registra las horas y calcula semanalmente Quién: responsable sistema biométrico.	**X**	
		Qué: Visación Cómo: Se revisa y aprueba el cálculo de horas para su pago. Cuándo: mensualmente Quién: Jefe de la Unidad de remuneraciones	**X**	
		El encargado de remuneraciones lleva un archivador con el detalle del las horas extras por funcionario		**X**

En este caso, se identifican tres controles mitigantes asociados directamente 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.

ANEXO Nº 10

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° 11 - 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°11 - 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 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.

Mayores antecedentes sobre esta materia también se pueden encontrar en el Documento Técnico N° 91: Conceptos Generales sobre Delitos Funcionarios, emitido por el CAIGG. Disponible en: http://www.auditoriainternadegobierno.cl.

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 mayor 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[31].

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.

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

[31] 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).

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 frecuentemente e injustificadamente se ausentan del lugar del

trabajo.

- Funcionarios públicos que, a menudo, se descuadran en 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° 69: Aseguramiento al Proceso de Compras Públicas, emitido por el Consejo de Auditoría Interna General de Gobierno (CAIGG), disponible en http://www.auditoriainternadegobierno.cl

ANEXO N° 14

SEÑALES DE ALERTA DE DELITOS 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.

CONSEJO DE AUDITORIA INTERNA GENERAL DE GOBIERNO

CAIGG

Ministerio Secretaría General de la Presidencia

ÁREA DE ESTUDIOS