



GOBIERNO DE SANTIAGO

**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE MODERNIZACIÓN, PLANIFICACIÓN ESTRATÉGICA
Y CONTROL DE GESTIÓN**

**APRUEBA POLÍTICA, DEFINICIÓN DE ROLES Y
RESPONSABLES, ROL AUDITORÍA INTERNA
EN EL PROCESO DE CONTROL INTERNO DE
RIESGOS ESTRATÉGICOS Y EL DICCIONARIO
DE RIESGOS**

RESOLUCIÓN EXENTA N°: 752

SANTIAGO, 22-04-2024

VISTOS:

El Acta de Proclamación del Tribunal Calificador de Elecciones de fecha 9 de julio de 2021; las facultades que me concede el artículo 24 letra ñ) de la Ley N°19.175 (08.11.2005) Orgánica Constitucional de Gobierno y Administración Regional y sus posteriores modificaciones; la Ley N°18.575 (05.12.1986) Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N°19.880 (29.05.2003) que establece las Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; Resoluciones Nos. 7/2019 y 16/2020, de la Contraloría General de la República; las Resoluciones Exentas N° 2.508 (14.12.2022), N°2.700 (30.12.2022), N°339 (24.02.2023) y N°4.245 (27.12.2023), que aprobaron la nueva Estructura Orgánica Funcional y Funciones del Servicio Administrativo del Gobierno de Santiago y la N°295 (15.02.2024) que crea el Comité de Control Interno de Riesgos Estratégicos.

CONSIDERANDO:

1. Que, el control interno es un proceso integral y dinámico que se adapta constantemente a los cambios que enfrenta la organización, es efectuado por la alta administración y las personas funcionarias de la entidad, está diseñado para enfrentar los riesgos y para dar una seguridad razonable del logro de la misión y objetivos de la entidad.

2. Que, el control interno es un proceso integral, consiste en una serie de acciones relacionadas con las operaciones de la entidad, que deben presentarse en forma continua y ser inherentes a la manera en que la alta dirección administra la organización. Debe ser diseñado dentro de las actividades propias de la entidad, de ese modo se vuelve parte integrada de los procesos de planificación, ejecución y seguimiento de la administración.

3. Que, el control interno debe ser efectuado por todas las personas funcionarias y colaboradores (as) del Gobierno de Santiago, porque no se trata solamente de manuales, políticas, sistemas y formularios, sino de personas y de las acciones que éstas aplican en cada nivel de la organización.



4. Que, el control interno es ejecutado tanto por la alta dirección como por el resto de los/as funcionarios(as) y colaboradores (as), incluida la función de auditoría interna, para ello, todas las personas deben conocer sus roles, responsabilidades, y los límites de autoridad existentes en la institución.

5. Que, el proceso de control interno conlleva al levantamiento de procesos estratégicos de la institución o la revisión de los mismos, la identificación, análisis y valoración de sus riesgos críticos y sus controles mitigantes y, en especial la formulación de medida de tratamiento de dichos riesgos estratégicos.

6. Que, la implementación del proceso de control interno de riesgos estratégicos debe tener presente el logro de la misión de la institución. Cualquiera sea la misión de la entidad, su consecución se enfrentará a toda clase de riesgos, por lo tanto, la tarea de la alta dirección es identificar y dar respuesta a ellos, por medio de un sistema de control interno robusto y conocido por toda la entidad.

7. Que, el Gobierno de Santiago es el organismo encargado de la administración superior de la Región, que tendrá por objeto el desarrollo social, cultural y económico de ella. En la administración interna de las regiones, los gobiernos regionales deberán observar como principio básico, el desarrollo armónico y equitativo de sus territorios, tanto en aspectos de desarrollo económico, como social y cultural.

8. Que, a su vez, en el ejercicio de sus funciones, deberán inspirarse en principios de equidad, eficiencia y eficacia en la asignación y utilización de recursos públicos y en la prestación de servicios, en la efectiva participación de la comunidad regional y en la preservación y mejoramiento del medio ambiente, para otorgar una mejor calidad de vida a los hombres y mujeres que viven en la Región.

9. Que, el proceso de control interno de riesgos estratégicos proporciona al Servicio la capacidad para gestionar todo el espectro de riesgos y posibilita que todo el personal mejore su comprensión del riesgo, y que para ello se debe establecer una política de control interno de riesgos estratégicos clara y precisa, que la defina.

10. Que, el proceso de control interno de riesgos estratégicos debe ser implementado en los distintos niveles de la organización, para lo cual se requiere una clara definición de roles y responsables en la implementación y desarrollo de éste.

11. Qué, la definición de roles y responsables implica definir, documentar y aprobar los roles claves de las personas relacionadas con las materias de prevención y reducción de los efectos de los riesgos estratégicos, control del tratamiento de los riesgos estratégicos, como asimismo, de identificar y registrar cualquier problema relacionado con el proceso de control interno de riesgos estratégicos, iniciar, recomendar o proveer soluciones a través de estrategias e igualmente, verificar a través del monitoreo la implementación de las soluciones contenidas en las estrategias.



GOBIERNO DE SANTIAGO

**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE MODERNIZACIÓN, PLANIFICACION ESTRATÉGICA
Y CONTROL DE GESTIÓN**

12. Que, se deben establecer y fomentar prácticas eficaces orientadas a prevenir la corrupción dentro de nuestra organización, tales como la implementación de sistemas de integridad y compliance.

RESUELVO:

1. **APRUEBESE** la Política, Definición de Roles y Responsables, Rol Auditoría Interna en el Proceso de Control Interno de Riesgos Estratégicos y el Diccionario de Riesgos (Anexos N°1, N°2, N°3 y N°4) que se adjuntan y forman parte integrante de esta Resolución.

2. **ASÍGNESE** a la Oficina de Auditoría Interna la función de auditar el funcionamiento y efectividad del Proceso de Control Interno de Riesgos Estratégicos, por lo que no podrá ser nombrada responsable en estos temas a fin de velar por su objetividad e independencia.

3. **DIFÚNDASE** el presente acto a todos los funcionarios del Gobierno Regional mediante su remisión vía correo electrónico.

Anótese, Regístrese, Comuníquese y Publíquese



FIRMADO

CLAUDIO ORREGO LARRAÍN

CARGO : GOBERNADOR REGIONAL

SERIE : 434252947977786441

MGS//JNS/CHM/VGT

Distribución :

- Administración Regional
- Jefaturas de División
- Jefaturas de Departamento
- Encargados de Unidad
- Funcionarios Gobierno de Santiago
- Oficina de Partes

ID DOC 127394

ANEXO N° 1

POLÍTICA CONTROL INTERNO DE RIESGOS ESTRATEGICOS

Visión general del Control Interno de Riesgos Estratégicos

El Gobierno de Santiago es el organismo encargado de la administración superior de la Región, que tendrá por objeto el desarrollo social, cultural y económico de ella. En la administración interna de las regiones, los gobiernos regionales deberán observar como principio básico, el desarrollo armónico y equitativo de sus territorios, tanto en aspectos de desarrollo económico, como social y cultural. A su vez, en el ejercicio de sus funciones, deberán inspirarse en principios de equidad, eficiencia y eficacia en la asignación y utilización de recursos públicos y en la prestación de servicios; en la efectiva participación de la comunidad regional y en la preservación y mejoramiento del medio ambiente.

Nuestra Misión:

Liderar, planificar y gestionar los asuntos públicos de la Región Metropolitana de Santiago hacia el desarrollo sustentable, social, cultural y económico de sus habitantes, garantizando la equidad, la transparencia y la responsabilidad en la asignación y utilización de los recursos, mediante una gobernanza participativa.

Nuestra Visión:

Seremos líderes en la gestión pública para el desarrollo de nuestra Región. Construiremos una ciudad metrópolis más competitiva, con mejores condiciones ambientales, mayores niveles de integración urbana, social y cultural, abasteciendo de servicios, infraestructura y equipamientos. Una capital sustentable, inclusiva, equitativa, moderna y segura.

Nuestros Valores:

Ética e Integridad: Los funcionarios y funcionarias del Gobierno de Santiago se comportan de manera íntegra, priorizando el interés público sobre los intereses particulares y siendo orientados por un conjunto de valores éticos. En este sentido, se busca mantener la rectitud y la honestidad de manera permanente en el ejercicio del cargo, luchando contra la corrupción.

Calidad y Generación de Valor Público: Los funcionarios y funcionarias del Gobierno de Santiago realizan una labor de calidad, velando por la eficiencia y eficacia en el uso de los recursos públicos. En este sentido, se desarrolla el valor público, entendido como el valor que la ciudadanía da a los bienes y servicios recibidos de la Institución cuando satisfacen oportunamente una necesidad.

Compromiso en el Servicio a las Personas: Los funcionarios y funcionarias del Gobierno de Santiago se comprometen a poner en el centro de su labor a las personas, priorizando su bienestar y un apropiado servicio público. En este sentido, tanto los objetivos, decisiones y actuaciones de la Institución se encuentran en armonía con las demandas de la ciudadanía.

Transparencia y Rendición de Cuentas: Los funcionarios y funcionarias del Gobierno de Santiago son transparentes en sus labores, cumpliendo con el derecho de acceso a la información que tienen las personas. En este sentido, la rendición de cuentas constituye un instrumento en virtud del cual se comunica a la ciudadanía el cumplimiento de los objetivos y metas de la Institución.

Respeto y Buen Trato: Los funcionarios y funcionarias del Gobierno de Santiago basan sus interacciones en el respeto y buen trato hacia todas las personas, sin existir discriminación arbitraria y velando por la inclusión social. En este sentido, basados en la cordialidad y deferencia hacia los demás, se consideran las ideas, opiniones y aspiraciones de todos y todas.

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

El mejoramiento de la gestión del Gobierno de Santiago está estrechamente relacionado con instalar un enfoque de gestión de calidad y excelencia que apunte a maximizar sus resultados y la satisfacción de sus destinatarios, sobre la base de la optimización de todos sus procesos de una manera integrada. A través del Modelo de Calidad de los Gobiernos Regionales se establecen los procesos para comenzar el camino hacia la excelencia. Los métodos que se aplican en este camino se basan en la relación entre los procesos estratégicos y sus resultados, según las siguientes premisas:

- Los procesos estratégicos producen resultados
- Los resultados dan cuenta de los procesos estratégicos

Por lo tanto, la mejora de los resultados se logra a través de la intervención en los procesos estratégicos que generan esos resultados. Instalar un enfoque y una cultura de mejoramiento continuo y de calidad y de excelencia en la gestión permite alcanzar estándares cada vez más exigentes, de una manera sistemática, logrando satisfacer crecientemente las necesidades y expectativas de todos los destinatarios, actores claves, ciudadanía, socios y colaboradores con un enfoque de calidad de servicio y satisfacción usuaria, un buen servicio en Gobierno de Santiago. En otras palabras, concebir la organización como un sistema que está en permanente adaptación a los desafíos del entorno.

Componentes del Control Interno de Riesgos Estratégicos

La creciente complejidad de los procesos estratégicos que se desarrollan en el Gobierno de Santiago, el entorno cambiante y la diversidad de aspectos involucrados, conllevan importantes riesgos, muchas veces producto de variables externas no controlables por el Servicio, a la cual se suman aquellos riesgos estratégicos inherentes a los procesos de gestión interna.

En este contexto, el Gobierno de Santiago considera necesario incorporar, como herramienta el proceso de control interno de riesgos estratégicos, la cual proporcionará al Servicio la capacidad para identificar, administrar, evaluar y gestionar los riesgos identificados en relación a sus recursos financieros, físicos y humanos, con el objetivo de minimizar el impacto negativo que se pueda presentar cuando ocurra cualquier eventualidad sobre los mismos, en función de la mejora continua de los resultados esperados.

Para ello, se instaló un proceso de control interno de riesgos estratégicos estructurado, consistente, integral y continuo, aplicado en los niveles estratégicos, tácticos y operacionales, que le permite al Servicio identificar, evaluar, medir y reportar amenazas que afectan el logro de los objetivos estratégicos, gestionar todo el espectro de riesgos y posibilitar que todo el personal mejore su comprensión del riesgo.

Lo anterior permite obtener:

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

Los lineamientos generales que orientan el proceso de control interno de riesgos estratégicos en el Gobierno de Santiago, son los siguientes:

1. Ejecutar las operaciones de manera ordenada, ética, económica, eficiente y efectiva.
2. Satisfacer las obligaciones de responsabilidad, en el sentido que tanto las organizaciones como las personas funcionarias que la integran, se hacen responsables por sus decisiones y acciones dentro de la misma.
3. Cumplir con las leyes y regulaciones vigentes.
4. Entregar protección a los recursos de la entidad contra pérdidas por mal uso, abuso, mala administración, errores, fraude e irregularidades. Así como también, para la información y documentación, que también corren el riesgo de ser mal utilizados o destruidos.
5. Enfocar la gestión en los procesos de mayor criticidad.

En el marco del proceso de control interno de riesgos estratégicos, el Gobierno de Santiago considera levantar los procesos estratégicos, los riesgos críticos y priorizarlos en función de la importancia relativa de cada uno de ellos, en el cumplimiento de su misión y objetivos estratégicos. Para ello, utilizará la metodología definida en las normas sobre control interno la Contraloría General de la República que consiste en el levantamiento de los procesos estratégicos del Servicio y su posterior priorización para luego ser tratados.

Entorno del Control Interno de Riesgos Estratégicos

El entorno de control establece la forma de dirigir una organización, teniendo plena injerencia en el conocimiento que tenga el personal sobre el control. Para establecer y mantener un entorno de control sólido en una entidad, se debe dar cumplimiento a los siguientes principios:

La organización demuestra compromiso con la integridad y los valores éticos: Las entidades tienen que mantener y demostrar integridad, la que debe hacer visible al público, a través de su misión y sus valores. La mantención de un estilo de dirección basado en dichos atributos debe considerar; una actitud de apoyo permanente hacia el control interno, independencia, sana competencia y liderazgo, un código de conducta establecido por la alta dirección, una evaluación del desempeño de las personas funcionarias que apoyen los objetivos de control interno y, en particular, de las operaciones éticas. Si la alta dirección de la entidad cree que el control interno es importante, los demás miembros de la organización responderán acatando los controles establecidos. La integridad personal y profesional, los valores éticos de la alta dirección y de las personas funcionarias que se desempeñan en la organización, se traduce en las normas de buena conducta.

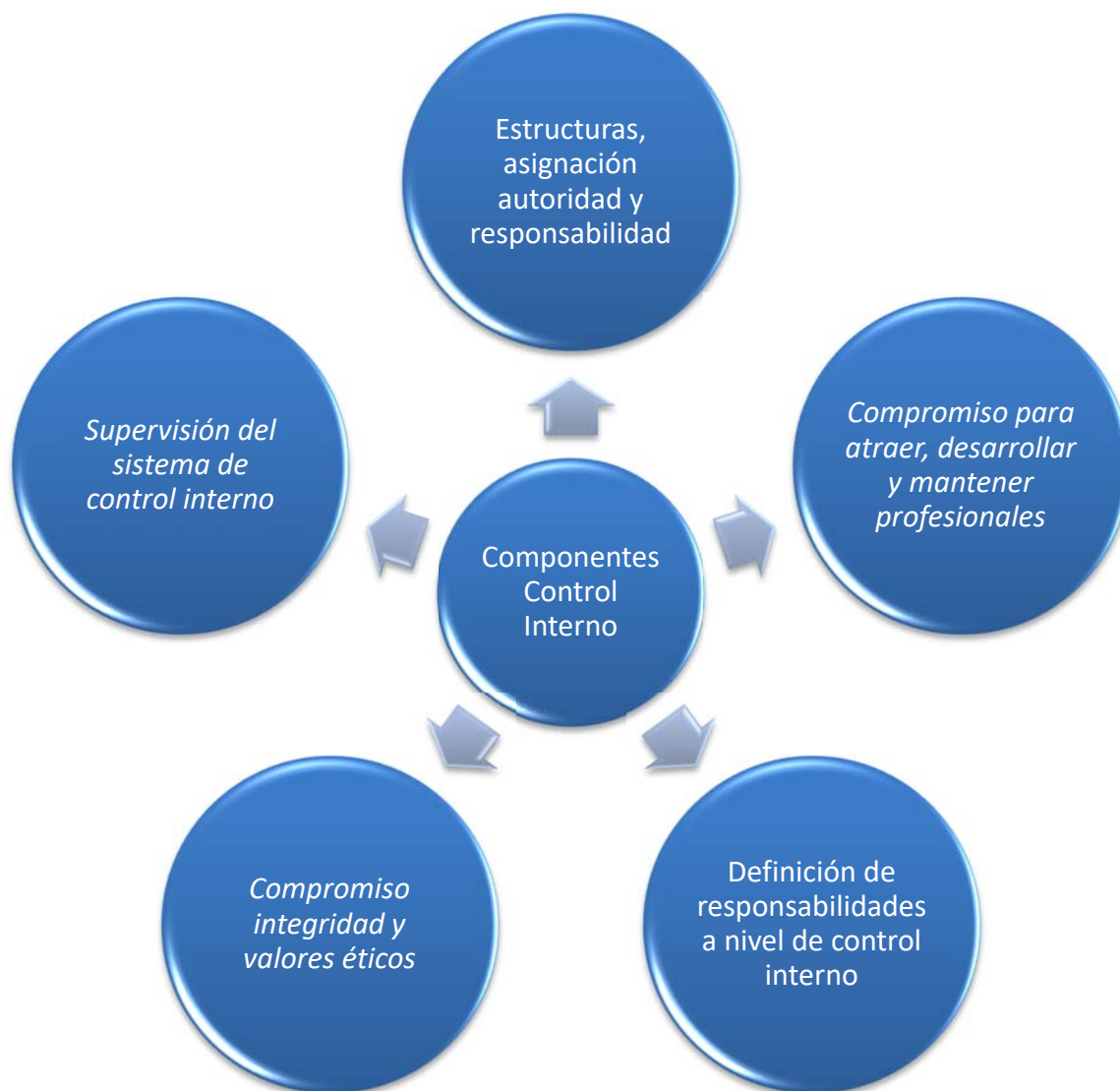
La máxima autoridad de la entidad ejerce la supervisión del desempeño del sistema de control interno: Corresponde a las máximas autoridades de la entidad la responsabilidad de supervisión del diseño, implementación y ejecución del sistema de control interno de la entidad. Para ello, dichas autoridades, deben definir, mantener y evaluar periódicamente las habilidades y los conocimientos necesarios de su equipo. Los conocimientos que se requieren deben considerar aspectos tales como conocimientos jurídicos y regulatorios que afectan el funcionamiento de la entidad.

Establecimiento de estructuras, asignación de autoridad y responsabilidad apropiadas para la consecución de los objetivos: La alta dirección de la entidad deberá establecer de manera formal, la estructura de la organización, considerando a todas las unidades que la conforman, además de definir las líneas de comunicación e información necesarias para planificar, ejecutar, controlar y evaluar periódicamente las actividades de la entidad, con la finalidad de llevar a cabo las responsabilidades de supervisión.

La organización demuestra compromiso para atraer, desarrollar y mantener profesionales competentes: El personal de una entidad constituye un factor importante del control interno, por ende, para un control efectivo, se necesita contar con personas funcionarias competentes. Para ello resulta necesario que los mecanismos de contratación del personal, las evaluaciones que se hacen, la capacitación, la promoción y la remuneración deben estar claramente establecidos a través de políticas o prácticas de recursos humanos. La capacitación constante puede aumentar la conciencia de las personas funcionarias sobre temas de control interno, probidad y ética.

La entidad define las responsabilidades de las personas funcionarias a nivel de control interno para la consecución de los objetivos: La responsabilidad por la rendición de cuentas en el ámbito del control interno hace referencia al compromiso que ha sido delegado a las personas funcionarias en aras de lograr los objetivos y teniendo en cuenta los riesgos a los que se enfrentan la organización.

Figura 1
Entorno del Control Interno de Riesgos Estratégicos



Evaluación de Riesgos Estratégicos

La evaluación de los riesgos es el proceso de identificación y análisis de los riesgos relevantes que pueden afectar el logro de los objetivos del Servicio, con el fin de determinar una respuesta apropiada para enfrentarlos. La identificación de los riesgos permite también asignar responsabilidades para el manejo de ellos.

Cualquiera sea la misión de la entidad, siempre se enfrentará a riesgos, por lo que la tarea de la alta dirección es identificarlos y dar respuesta a éstos con el objeto de maximizar la posibilidad de alcanzar tanto la misión definida, como los objetivos generales de la organización.

Para que el proceso de identificación y evaluación de los riesgos sea efectivo, se deben considerar los siguientes principios:

- 1. Definir los objetivos de la entidad con suficiente claridad para permitir la identificación y evaluación de los riesgos.**

La alta dirección debe definir los objetivos operacionales, de información y de cumplimiento.

- a) **Objetivos operacionales:** Reflejan las decisiones efectuadas por la máxima autoridad de la entidad respecto 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.
- b) **Objetivos de información:** Esta categoría considera la información financiera y no financiera tanto externa como interna. Los objetivos de información externa, se originan principalmente en las leyes y normativas establecidas por los entes reguladores, y los objetivos de información interna, se determinan a partir de las instrucciones estratégicas de la organización.
- c) **Objetivos de cumplimiento:** Estos objetivos reflejan las leyes y regulaciones externas de la entidad, asimismo, se deben considerar los niveles aceptables de variación para dar cumplimiento a estos objetivos.

Al momento de confirmar la idoneidad de los objetivos, la alta dirección puede considerar aspectos tales como evaluar si se alinean con las prioridades estratégicas de la organización, y con las leyes, regulaciones y normas aplicables a la entidad; adicionalmente, se debe tener en consideración que los objetivos deben desplegarse a todos los niveles de la organización y sus unidades.

2. Identificar los riesgos para la consecución de los objetivos en todos los niveles de la organización, y análisis para determinar cómo se pueden mitigar.

El proceso de identificación de riesgos deberá considerar todos los procesos que se desarrollen en la entidad, abarcando además la totalidad de las interacciones o relaciones que se generen en ellos.

Este proceso deberá considerar, a lo menos:

- a) Identificación de riesgos a nivel de la entidad.

Los riesgos a nivel de organización pueden derivar tanto de factores internos y/o externos, entre los cuales se pueden mencionar:

Factores externos:

Económicos: Se refiere a cambios que podrían afectar la cantidad y forma de percibir los recursos monetarios, por ejemplo, el aumento o disminución del tipo de cambio, o valor de la UF, entre otros.

Entorno natural: Considerar aspectos como catástrofes naturales, cambios en el clima que podrían afectar las operaciones regulares de la organización o dañar los activos que dispone.

Regulatorios: Cambios en el marco normativo que podrían significar modificaciones en la función que cumple la entidad, restricciones en el uso de sus activos, entre otros.

Sociales: Las expectativas y necesidades cambiantes de los(as) usuarios(as) podrían afectar al desarrollo de las prestaciones que otorga.

Tecnológicos: Avances que podrían afectar la disponibilidad, el procesamiento y el uso de datos.

Factores internos:

Infraestructura: Decisiones respecto al uso de bienes que podrían afectar las operaciones que desarrolla la entidad y el logro de sus objetivos.

Estructura de la dirección: Cambios en las responsabilidades de la dirección de la entidad, que puedan afectar como se ejecutan determinados controles.

Personal: Se refiere a la calidad del personal contratado y a los métodos de formación y motivación que puedan influir en el control dentro de la entidad.

Acceso a activos: Actividades que realiza la organización y la accesibilidad de las personas funcionarias a los activos que mantiene.

Tecnología: Interrupciones en el procesamiento de los sistemas de información podrían afectar negativamente al funcionamiento de la organización.

b) Identificación de riesgos a nivel de transacción.

El proceso de identificación de riesgos a nivel de transacciones considera los riesgos existentes dentro de sus distintas divisiones, direcciones, departamentos o unidades, incluidos los procesos de negocio, tales como ingresos, adquisiciones, recursos humanos, finanzas, entre otros.

c) Análisis de los riesgos identificados.

Una vez que se han identificado los riesgos, tanto a nivel de entidad como a nivel de transacción, se debe analizar la probabilidad de que se materialice dicho riesgo y el impacto de su ocurrencia en la entidad. A través de tal evaluación, los riesgos podrían tener rangos para establecer prioridades para la alta administración y las correspondientes decisiones asociadas.

d) Definición del nivel de tolerancia al riesgo en una organización.

La “tolerancia al riesgo” es la cantidad de riesgo a la que una entidad está preparada para exponerse antes de determinar que una acción deba ser tomada. Para determinar dicha tolerancia se deben considerar tanto los riesgos inherentes, definido como “aquel que afecta a la consecución de los objetivos de la organización en caso de que no concurren medidas por la dirección para alterar la probabilidad o el impacto del riesgo”, como los riesgos residuales, definido como “aquel que afecta la consecución de los objetivos y que sigue existiendo una vez adoptadas e implementadas las respuestas pertinentes por parte de la organización”.

Con todo, el análisis de riesgos se aplica primero al riesgo inherente, y posteriormente, una vez efectuada la respuesta al riesgo, se analiza el riesgo residual, debiendo considerarse ambos para comprender hasta qué punto se necesitan adoptar respuestas ante dichos riesgos.

e) Desarrollo de las respuestas a los riesgos.

El resultado de las acciones arriba mencionadas puede resultar en un mapa o matriz de riesgo para la organización. Habiendo desarrollado un mapa de riesgo, la organización puede entonces considerar las respuestas apropiadas para administrarlo.

El propósito de la administración del riesgo no es necesariamente evadir el riesgo, sino mantenerlo bajo control. Los procedimientos que una organización establece para tratar el riesgo se llaman actividades de control.

Figura 2
Evaluación de Riesgos Estratégicos



3. Considerar la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.

La evaluación de riesgos deberá incluir la valoración de aquellos relativos a la información fraudulenta, pérdida de activos y casos de corrupción en la organización.

La evaluación del riesgo de fraude debe tener en consideración los incentivos y las presiones a las que podrían estar expuestas las personas funcionarias para participar o justificar actuaciones irregulares. Las oportunidades surgen como resultado de débiles actividades de control y supervisión, por una deficiente vigilancia por parte de la dirección y por la elusión de los controles por parte de la misma.

Es posible mitigar la probabilidad de un riesgo relacionado con el fraude mediante la adopción de medidas dentro de otros componentes del control interno o realizando cambios en las unidades operativas, procesos de negocio y actividades de la organización.

4. Identificar y evaluar los cambios que podrían afectar significativamente al sistema de control interno.

Es fundamental para la evaluación de riesgos la existencia de un proceso permanente para identificar el cambio en las condiciones económicas, industriales, regulatorias y operativas que afecten la entidad, y tomar las acciones necesarias para enfrentarlas.

Para ello, los perfiles de riesgo y controles relacionados tienen que ser regularmente revisados y adecuados para asegurar que el mapa del riesgo sigue siendo válido.

Adicionalmente, se deben considerar riesgos relacionados a cambios en el personal, por ejemplo, un miembro nuevo(a) de la alta dirección puede que no comprenda la cultura de la entidad y refleje una filosofía diferente, lo que puede afectar al resto de las personas funcionarias.

Actividades de control interno de riesgos estratégicos

Las actividades de control corresponden a las políticas y procedimientos establecidos y ejecutados en dirección a minimizar los riesgos, para lograr con ello los objetivos de la entidad.

Las actividades de control para ser efectivas, deben ser apropiadas, funcionar consistentemente de acuerdo a un plan, por un período de tiempo, y tener un costo adecuado. Para ello, se deben considerar los siguientes principios:

1. Definir y desarrollar actividades de control que contribuyan a la mitigación de los riesgos hasta niveles aceptables.

Para dar cumplimiento a este principio se debe tener presente lo siguiente:

- a) Integración con el componente de evaluación de riesgos: Una vez que la dirección identificó y evaluó los riesgos, la entidad pondrá en marcha las acciones necesarias para llevar a cabo respuestas a los riesgos específicos a través de las actividades de control.
- b) Factores específicos de la organización: Se deben considerar aquellos elementos que puedan afectar a las actividades de control, tales como el entorno y la complejidad de una entidad, la regulación, los sistemas informáticos utilizados, así como el tipo de estructura de las operaciones (centralizada o descentralizada).
- c) Determinar los procesos de negocio relevantes: La dirección deberá tener en cuenta los procesos de negocio relevantes, las tecnologías de información y las etapas de los procesos en los que se necesitan actividades de control.
- d) Tipos de actividades de control: Las actividades de control pueden ser preventivas o detectivas, siendo normalmente utilizadas una combinación de ambos tipos. La principal diferencia entre ambas es el momento en el que se produce la actividad de control. Un control preventivo está diseñado para evitar un evento o resultado no previsto en el momento en el que se produce por primera vez, mientras que un control de detección está diseñado para identificar un evento o resultado no previsto después de que se haya producido el procesamiento inicial. Adicionalmente, las actividades de control pueden ser efectuadas de forma manual, automática (utilizando sistemas informáticos) o una mezcla de ambos.

A continuación, se presentan actividades de control:

✓ Controles preventivos:

Autorización y aprobación: Confirma que una transacción es válida, es decir, representa un evento real o que se encuentra dentro de la política de la entidad, además es efectuada sólo por personas que estén dentro del rango de autoridad. Los procedimientos de autorización tienen que ser documentados y claramente comunicados a las jefaturas y personas funcionarias.

Controles de acceso a los recursos y archivos: Debe ser limitado a las personas funcionarias autorizadas que sean responsables por la custodia y/o utilización de los mismos. La responsabilidad en cuanto a la custodia se pone en evidencia a través de la implementación de comprobantes, realización de inventarios y otros registros. La restricción de acceso a los recursos reduce el riesgo de utilización no autorizada, adulteración o pérdida.

Segregación de funciones: Es la asignación y división de responsabilidades de registrar, autorizar y aprobar transacciones, así como de administrar los bienes y activos en una entidad.

✓ **Controles detectivos:**

Verificaciones: Revisión de transacciones después de ser procesadas, por ejemplo: cuando los bienes son entregados, el número de bienes provistos es verificado con el número de bienes solicitados.

Conciliaciones: Los archivos deben ser conciliados con los documentos que correspondan, por ejemplo, los archivos de contabilidad relacionados con las cuentas corrientes bancarias son conciliados con los saldos bancarios correspondientes a determinada data.

Revisión de desempeño: El desempeño de las operaciones es revisado de acuerdo a las normas o procedimientos establecidos, evaluando la efectividad y eficiencia de las mismas.

Análisis o monitoreo general: Actividades de control que operan de manera más generalizada o más amplia, como, por ejemplo, revisiones analíticas o análisis del desempeño a nivel de entidad.

2. Definir y desarrollar actividades de control generales de tecnología para apoyar el logro de los objetivos.

Se debe establecer la dependencia entre el uso de la tecnología y los controles generales sobre la misma, es decir, la confiabilidad y seguridad de los sistemas informáticos que procesan, mantienen y reportan información relevante en el sistema de control interno.

Los controles generales sobre la tecnología incluyen actividades de control sobre las infraestructuras tecnológicas, la gestión de la seguridad, y la adquisición, desarrollo y mantenimiento de tecnologías. Dichos controles son aplicables a todo tipo de tecnologías, desde aplicaciones sofisticadas hasta entornos de escritorio, de usuario final y dispositivos móviles.

3. Desplegar actividades de control a través de políticas y procedimientos.

- a) Las políticas reflejan la visión de la dirección sobre lo que debe hacerse para llevar a cabo el control, mientras que los procedimientos se componen de medidas que implementan una política. La implementación de políticas y procedimientos debe considerar:
- b) Respalda la implementación de las instrucciones adoptadas por la alta administración en los procesos de negocios y de las actividades de las personas funcionarias dependientes de la entidad.
- c) Expresarse por escrito y ser comunicados a todas las personas de la organización que se vean involucrados en el proceso.
- d) Establecer responsabilidades que asumirá el personal que lleve a cabo cada actividad de control en relación con la ejecución de políticas y procedimientos.
- e) Incluir el plazo en que una actividad de control debe ejecutarse y las medidas correctivas de seguimiento que deben ser llevadas a la práctica, para controlar la efectividad del control.
- f) Adoptar medidas correctivas en aquellos casos en que la aplicación de las actividades de control se identifiquen situaciones que deban ser investigadas y seguidas, definiendo al personal que investigará.
- g) Actividades ejecutadas por personal competente.
- h) Reevaluación permanente tanto de las políticas como de los procedimientos y las actividades de control que se implementen, con independencia de la capacidad que mantenga la entidad de dar respuesta a los cambios significativos que se susciten en los riesgos identificados o en los objetivos definidos por la organización.

Información y Comunicación

La información y la comunicación son esenciales para ejecutar todos los objetivos de control interno, para ello las entidades deben ceñirse a los siguientes principios:

1. La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.

La información es necesaria para que la organización pueda llevar a cabo sus responsabilidades de control interno en aras de conseguir sus objetivos, para ello, el sistema de control interno como tal y todas las transacciones y eventos significativos deben estar apropiadamente documentados a través de sistemas de información.

Un sistema de información es un conjunto de actividades, que considera personas, procesos, datos y/o tecnologías, y que permite a la entidad obtener, generar, utilizar y comunicar transacciones e información para mantener la adecuada responsabilidad por la rendición de cuentas; medir y revisar el desempeño de la organización; y el avance en la consecución de los objetivos.

La capacidad de generar información de calidad comienza con el análisis de los datos relevantes, por cuanto si se dispone de datos poco precisos o incompletos, la información derivada puede provocar que se adopten decisiones equivocadas, que se efectúen estimaciones erróneas o que se aplique de manera deficiente el criterio profesional de la alta dirección de la entidad.

2. La organización comunica internamente los objetivos y responsabilidades necesarias para el sistema de control interno.

La información es la base de la comunicación, debe darse en todas las direcciones y llegar a todos los componentes de la estructura de la entidad. Para ello, la alta dirección debe:

- Estar actualizada en cuanto a la actuación, desarrollo, riesgos y funcionamiento del control interno.
- Comunicar a su personal la información que requiere retroalimentación y dirección.
- Proveer comunicación específica y dirigida, relacionada con las expectativas de la conducta de las personas funcionarias.

La comunicación debe elevar la conciencia sobre la importancia y la relevancia de un control interno efectivo, comunicar la tolerancia al riesgo de la entidad, y hacer que el personal esté consciente de su rol y responsabilidades al efectuar y apoyar los componentes del control interno.

3. La organización comunica a las partes interesadas externas los aspectos claves que afectan al funcionamiento del control interno.

La alta dirección debe asegurar que existan medios adecuados para comunicarse y obtener información de las partes relacionadas externas, por cuanto dicha información es insumo para el logro de sus propios objetivos. Los controles que facilitan la comunicación externa pueden ser políticas y procedimientos para obtener o recibir información procedente de grupos de interés externos.

Seguimiento y/o actividades de supervisión

El proceso de seguimiento del control interno busca asegurar que los controles funcionen adecuadamente y que sean modificados de acuerdo a los cambios en las condiciones en las que operan las instituciones.

El seguimiento debe asegurar que se alcanzan los objetivos generales expuestos en la definición de control interno de la entidad y distinguirse claramente de la revisión de las operaciones diarias de la misma. Para lograr un seguimiento efectivo, se debe dar cumplimiento a los siguientes principios:

1. Realizar evaluaciones continuas y/o puntuales para determinar si los componentes del sistema de control interno están presentes y en funcionamiento.

Las actividades de evaluación continua, puntuales o una combinación de ambas, permiten asegurar que el control interno siga siendo aplicable a todos los niveles y en toda la entidad, logrando los resultados deseados.

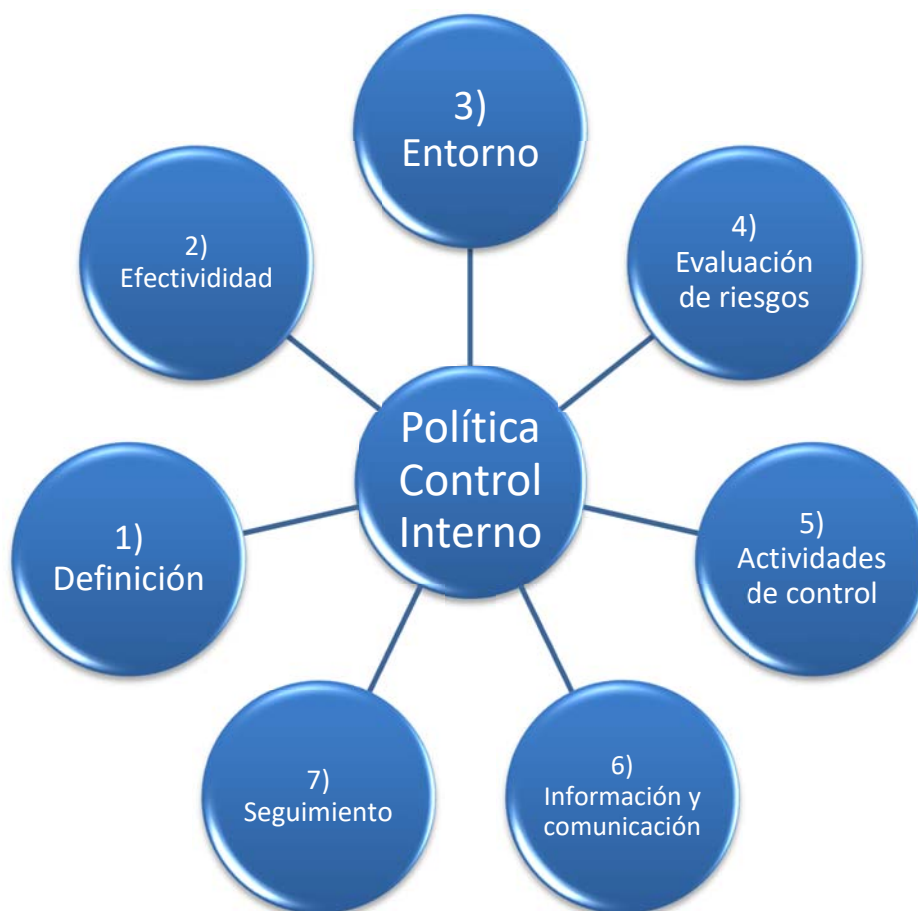
2. Evaluar y comunicar las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas incluyendo la alta dirección.

Todas las deficiencias o hallazgos encontrados durante las evaluaciones continuas y/o puntuales deben ser comunicadas a las personas funcionarias responsables que puedan tomar las acciones correctivas necesarias y en forma oportuna.

Para ello, las personas funcionarias responsables de cada proceso en la entidad, incluida la alta dirección, deben:

- Evaluar oportunamente los hallazgos, así como también, las recomendaciones que pudieran entregar los(as) auditores(as) u otros que evalúen las operaciones de las unidades/departamentos de la entidad.
- Determinar las acciones correctivas en respuesta a los hallazgos y recomendaciones de las auditorías y/o revisiones efectuadas.
- Implementar, dentro de los marcos establecidos, todas las acciones que corrijan o resuelvan los asuntos que han llamado la atención.

Figura 3
Política Control Interno de Riesgos Estratégicos



ANEXO N° 2

DEFINICIÓN DE ROLES Y RESPONSABLES DEL CONTROL INTERNO DE RIESGOS ESTRATÉGICOS

El control interno debe ser efectuado en primer lugar por la propia entidad, es decir, la alta dirección, el personal y los(as) auditores(as) internos(as). Si bien, todos tienen participación en el sistema de control interno, la alta dirección es la principal responsable de su aplicación y cumplimiento, el cual es necesario para un eficiente y adecuado proceso operativo.

Por otra parte, están las acciones de control que ejercen las partes interesadas externas que también tienen impacto en el sistema de control interno de la entidad, como por ejemplo la Contraloría General, y otros actores que tienen influencia en el cumplimiento de los objetivos de la entidad.



1. Alta dirección (1era línea de control)

La alta dirección, es la primera línea de control de una entidad y tiene la responsabilidad general del diseño, implementación y supervisión del correcto funcionamiento, mantenimiento y documentación del sistema de control interno. La administración superior de la entidad puede incluir Jefes(as) de Servicio, Alcaldes y Alcaldesas, Directivos(as), u otros definidos por la propia entidad.

La alta dirección debe tener asumido que una sólida estructura de control interno es primordial para el cumplimiento de sus propósitos. Asimismo, permite contribuir a mejorar a las operaciones de la organización, evaluando y mejorando la eficacia de los procesos de gestión de riesgos, control y gobierno.

Algunos ejemplos de las actividades que debe efectuar la alta dirección son:

- Propiciar un ambiente ético en la organización, por ejemplo, estableciendo un código de ética y de conducta.
- Definir áreas de autoridad y responsabilidad formales y darlas a conocer al resto de las personas funcionarias.

- Establecer personal con competencias adecuadas para cumplir dichas funciones.
- Establecer un sistema de control de calidad en la organización.
- Asegurar la competencia profesional del personal de auditoría interna.
- Implementar un sistema de aseguramiento de la calidad de los procesos de la organización.

2. Personas funcionarias (2da línea de control)

Las personas funcionarias de una entidad que no son parte de la alta dirección, tales como jefaturas intermedias, encargados(as), coordinadores(as) y otras personas funcionarias, tiene un rol relevante en el cumplimiento del control interno. Muchas veces son las personas funcionarias las que aplican, revisan y/o corrigen las actividades de control implementadas en los diversos procesos de una organización, identificando en la práctica qué aspectos pueden ser mejorados a través de los controles.

Algunos ejemplos de las actividades que deben efectuar las personas funcionarias son:

- Efectuar las labores diarias con apego a los planes y procedimientos internos.
- Reportar a las jefaturas anomalías en las actividades de control que pudieran afectar el cumplimiento de los objetivos institucionales.

3. Auditoría Interna (3ra línea de control)

Los(as) auditores(as) internos(as) forman parte importante del marco de control interno de una organización, sin embargo, no son los responsables de la aplicación de procedimientos específicos de control, asimismo, la auditoría interna como tal no puede reemplazar la existencia de un sólido y adecuado sistema de control interno.


La alta dirección, debe utilizar la labor de la auditoría interna como ayuda para el monitoreo de la efectividad del control interno, por cuanto proporciona información continua sobre el funcionamiento, de la entidad y la evaluación del diseño y operación del control interno, pudiendo entregar recomendaciones para mejorar las debilidades detectadas, sin dejar nunca de lado la independencia y la objetividad.

4. Contraloría General de la República (4ta línea de control)

La función de la Contraloría General es contribuir en el logro de los objetivos de la entidad y proveer información útil para llevar a cabo adecuados procedimientos de control interno.

Conforme lo ha establecido su mandato⁸, la Contraloría General evaluará los sistemas de control interno de las entidades; fiscalizará la aplicación de las disposiciones relativas a la administración financiera del Estado, particularmente, las que se refieren a la ejecución presupuestaria de los recursos públicos; examinará las operaciones efectuadas y la exactitud de los estados financieros; comprobará la veracidad de la documentación sustentatoria; verificará el cumplimiento de las normas estatutarias aplicables a las personas funcionarias públicas y formulará las proposiciones que sean adecuadas para subsanar los vacíos que detecte, informando de ello a la alta dirección. Lo anterior a través de la ejecución de auditorías o investigaciones especiales.

Figura
Definición de roles y responsables del Proceso de Control Interno de Riesgos Estratégicos

ESTRUCTURA ORGANIZACIONAL COMITÉ DE CONTROL INTERNO DE RIESGOS ESTRATEGICOS	RESPONSABLES	ROLES CLAVES
	<u>Jefe/a de Servicio</u> ❖ Gobernador de Santiago	✓ Promover la gobernanza a través de la transparencia y la rendición de cuentas para el uso de los recursos públicos
	<u>Encargado/a de Riesgos Estratégicos</u> ❖ Jefatura División Administración y Finanzas	✓ Presidir y coordinar el Comité de Control Interno de Riesgos Estratégicos
	<u>Secretaría Ejecutiva del Comité</u> ❖ Jefatura Departamento de Modernización, Planificación Estratégica y Control de Gestión	✓ Rendir cuenta al Comité de Control Interno de Riesgos Estratégicos del Proceso ✓ Actualizar o mantener la gobernanza del Proceso de Control Interno de Riesgos Estratégicos ✓ Determinar la matriz de evaluación de Riesgos Estratégicos ✓ Establecer el plan de tratamiento de Riesgos Estratégicos
	<u>Comité de Control Interno de Riesgos Estratégicos*</u> ✓ Gobernador/a ✓ Administrador/a Regional ✓ Jefaturas de División ✓ Jefatura Unidad de Control Interno ✓ Jefatura Departamento Jurídico y Fiscalía ✓ Jefatura Departamento de Modernización, Planificación Estratégica y Control de Gestión ✓ Jefatura Departamento de Finanzas ✓ Jefatura Departamento de Gestión de Abastecimiento ✓ Jefatura Departamento de Inversiones ✓ Jefatura Departamento de Presupuesto ✓ Jefatura de Control de Programas ✓ Jefatura Departamento de Normalización y Gestión ✓ Jefatura Departamento de Análisis y Evaluación de Inversiones ✓ Jefatura Departamento de Tecnologías de la Información	✓ Supervisar la implementación del Proceso de Control Interno de Riesgos Estratégicos ✓ Liderar y coordinar el Proceso de Control Interno de Riesgos Estratégicos ✓ Analizar el avance y desarrollo de las medidas de mitigación del plan de tratamiento de riesgos estratégicos

	<p><i>* Puede concurrir el titular o un suplente</i> <u>Los Coordinadores de Riesgos Estratégicos serán los siguientes miembros:</u></p> <ul style="list-style-type: none"> ✓ Representante Departamento de Análisis y Evaluación de Inversiones ✓ Representante Departamento de Presupuesto ✓ Representante División de Desarrollo Social y Humano ✓ Representante División de Fomento e Industria ✓ Representante División de Infraestructura y Transportes ✓ Representante Departamento de Seguridad Ciudadana ✓ Representante Departamento de Medio Ambiente, Biodiversidad y Acción Climática ✓ Representante Departamento Jurídico y Fiscalía ✓ Representante Departamento de Gestión de Abastecimiento ✓ Representante Departamento de Inversiones ✓ Representante Departamento de Control de Programas ✓ Representante Departamento de Finanzas 	<ul style="list-style-type: none"> ✓ Revisar y actualizar, según aplique, anualmente el levantamiento de información de procesos, riesgos críticos y controles claves existentes ✓ Implementar las medidas de mitigación del plan de tratamiento de riesgos estratégicos ✓ Rendir cuenta de las medidas de mitigación del plan de tratamiento de riesgos estratégicos
--	---	--

ANEXO N° 3

ROL DE LA OFICINA DE AUDITORIA INTERNA EN EL PROCESO DE CONTROL INTERNO DE RIESGOS ESTRATEGICOS

El Gobierno de Santiago cuenta con un proceso de control interno de riesgos estratégicos, por tanto, se formula y actualiza la Matriz de Control Interno de Riesgos Estratégicos y las estrategias para tratar y monitorear los riesgos, todos estos elementos pasan a formar parte de lo que debe considerar la Oficina de Auditoría Interna en su planificación y programación.

La auditoría interna debe ser una actividad independiente dentro de la organización, de garantía objetiva y carácter consultor que agregue valor y mejore el funcionamiento de la entidad, además debe tener independencia de las operaciones regulares de la entidad, reportando sus resultados a la autoridad máxima de la organización. Esto último, permite que se presenten opiniones imparciales respecto de la valoración del control interno, con propuestas objetivas que busquen corregir las anomalías detectadas.

Por otra parte, la auditoría interna puede contribuir a la eficiencia de las tareas realizadas por auditores(as) externos(as), tanto de la Contraloría General como de firmas auditoras privadas (si es aplicable), por cuanto, la naturaleza y alcance de los procedimientos establecidos por la auditoría externa pueden ser modificados si se confía en el trabajo del(a) auditor(a) interno(a) y en la eficiencia de los controles implementados en la organización.

Algunos ejemplos de las actividades que debe efectuar la Oficina de Auditoría Interna son:

- Asesorar a la gerencia en áreas en riesgo.
- Establecer planes y objetivos estratégicos periódicos de auditoría.
- Realizar auditorías a las operaciones de la entidad.
- Evaluar los sistemas de tecnología de la información utilizados.
- Recomendar formas de mejorar las operaciones y fortalecer los controles.
- Hacer seguimiento de las recomendaciones con el fin de constatar que sean completa y efectivamente implementadas.
- Coordinar las actividades de auditoría con los(as) auditores(as) externos(as).

Los beneficios de la coordinación y la cooperación con los auditores(as) internos(as), pueden contribuir entre otros, a lo siguiente:

- Fortalecimiento de la capacidad mutua de promover la gobernanza y las prácticas de rendición de cuentas y así mejorar la comprensión, por parte de la gestión, de la importancia del control interno.
- Auditorías más eficientes enfocada en los riesgos que enfrenta la organización, enfocándose en aspectos que afectan el funcionamiento de la entidad y, por lo tanto, con recomendaciones útiles.
- Mejorar la comprensión de los resultados que surjan del trabajo del otro, el cual podría tener un impacto en los planes de auditorías futuros.
- Minimizar la interrupción de las funciones de la entidad auditada.
- Mejorar y maximizar la cobertura de la auditoría basada en evaluaciones de riesgos e identificación de riesgos significativos.

ANEXO N° 4

DICCIONARIO DE RIESGOS

A

Aceptar el Riesgo: Una de las estrategias globales para tratar los riesgos de una organización, que consiste en No emprender 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).

Administración de Riesgos: Ver Proceso de Gestión de Riesgos.

Acción Correctiva: Las acciones tomadas por la administración basadas en la retroalimentación de los resultados de una auditoría o acción de control.

Análisis de Costo-Beneficio: Es una herramienta que se utiliza en el proceso de gestión de riesgos, para orientar la toma de decisiones sobre las estrategias y acciones para el tratamiento de los riesgos.

Actitud ante el Riesgo: Enfoque de la organización para evaluar un riesgo y eventualmente buscarlo, retenerlo, tomarlo o rechazarlo.

Actividades de Control: Componente del Marco Integrado de Control Interno, se refiere a las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones del Jefe de Servicio para mitigar los riesgos con impacto potencial en los objetivos.

Actividades de Supervisión: Componente del Marco Integrado de Control Interno, se refiere a las evaluaciones continuas y las evaluaciones independientes o una combinación de ambas, se utilizan para determinar si cada uno de los cinco componentes del control interno, incluidos los controles para cumplir los principios de cada componente, están presentes y funcionan adecuadamente.

Administración de Riesgos: Ver Proceso de Gestión de Riesgos.

Apetito de Riesgo: Es la cantidad de riesgo a nivel global, que la administración está dispuesto a aceptar en su búsqueda de valor. Este puede ser establecido en relación a la organización como un todo, para diferentes grupos de riesgos o en un nivel de riesgo individual. (Ver riesgo aceptado).

Aseguramiento: Un sistema de gobierno corporativo que provee retroalimentación acerca de la eficacia de las operaciones, acatamiento con las leyes y las regulaciones, y la precisión y seguridad de la información financiera.

Aseguramiento del Proceso de Gestión de Riesgos: Actividad independiente y objetiva de aseguramiento sobre la efectividad del Proceso, que realiza la Unidad de Auditoría Interna, de acuerdo con las directrices del Consejo de Auditoría. Este proceso de retroalimentación ayudará a asegurar que los riesgos claves de negocio sido identificados en forma adecuada y están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente.

Auditoría Interna: La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Auditoría Basada en Controles: Auditorías que usan el sistema de control interno como su objetivo de la auditoría, centrándose en priorizar áreas funcionales importantes, revisar controles relevantes, determinar debilidades en los controles, sugerir mejoramiento de controles débiles y determinar grado de implementación y reforzamiento de controles.

Auditoría Basada en Riesgos: Auditorías que se enfocan en el riesgo y administración de riesgos como el objetivo de la auditoría, centrándose en priorizar procesos riesgosos y estratégicos, evaluar riesgos relevantes y determinando la eficiencia de los controles asociados a riesgos, analizando los riesgos y emitiendo recomendaciones para mitigarlos.

Auto-Evaluación de Controles (Control Self-Assessment): eSA abreviada. Una clase de métodos usada en una auditoría o en lugar de una auditoría para evaluar la fuerza y la debilidad de los riesgos y los controles versus una estructura de control. La "auto" evaluación se refiere a la participación de la dirección y el personal en el proceso de la evaluación, muchas veces ayudados por los auditores internos. Los métodos eSA incluye talleres, seminarios, grupos de enfoque, entrevistas estructuradas, y cuestionarios de encuesta.

C

Capacidad de Riesgo: Cantidad y tipo de riesgo máximo que una organización es capaz de soportar en la persecución de sus objetivos.

Cartera de Riesgos: Este concepto asume que varios riesgos comparten ciertas características y/o interdependencias. Los riesgos son considerados en grupos, basados en cómo ellos se relacionan unos con otros, y dentro de esos grupos uno o más riesgos pueden aparecer o desaparecer cuando otros riesgos aparecen o desaparecen.

Catastrófico: Es un evento negativo o riesgo cuya materialización influye gravemente en el desarrollo del proceso y en el cumplimiento de sus objetivos, impidiendo finalmente que éste se desarrolle.

Categorías de Objetivos: El Marco Integrado de Control Interno establece tres categorías de objetivos, que permiten a las organizaciones centrarse en diferentes aspectos del control interno: Objetivos Operacionales, Objetivos de Información y Objetivos de Cumplimiento.

- o **Objetivos Operacionales:** Hacen referencia a la eficacia y eficiencia de las operaciones de la organización, incluidos sus objetivos de desempeño, financieros y operativos, y la protección de sus activos frente a posibles pérdidas.
- o **Objetivos de Información:** Hacen referencia a la información financiera y no financiera interna y externa, y pueden abarcar aspectos de fiabilidad, oportunidad, transparencia u otros conceptos establecidos por los reguladores, organismos de normalización o por las políticas de la propia organización gubernamental.
- o **Objetivos de Cumplimiento:** Hacen referencia al cumplimiento de las leyes y regulaciones a las que está sujeta la organización gubernamental.

Causa: Factor externo o interno que genera un riesgo.

Clasificación (Ranking): El proceso de establecer el orden o la prioridad en base a criterios definidos.

Clasificación Comparativa de Riesgos: Uso de criterios para diferenciar cuáles son los riesgos altos y bajos.

Clasificación de Riesgos: La categorización del nivel de severidad del riesgo de acuerdo a criterios de valoración predefinidos (por ejemplo; Extremo, Alto, Moderado y Bajo).

Conflicto de Interés: Situaciones (potenciales, reales o aparentes), en las que un asunto privado o motivación personal puede influir indebidamente en el correcto ejercicio de sus funciones y en la toma de decisiones objetivas. Por ejemplo, favorecer en una licitación a una amistad o participar en la selección de un cargo en la que postula un familiar.

Consecuencia: Ver Impacto.

Compartir el Riesgo: Una de las estrategias globales para tratar los riesgos de una organización, que consiste en trasladar o distribuir las posibles consecuencias de riesgos dentro de varios grupos. Los seguros y otros contratos son algunos de los métodos usados para compartir o transferir riesgos.

Contexto de Gestión de Riesgos: Definición del alcance de aplicación, los criterios de evaluación y la estructura del análisis de los riesgos que se utilizarán en el Proceso de Gestión de Riesgos.

Contexto Externo: Entorno en el que opera la organización, considerando aspectos tales como los financieros, operacionales, competitivos, políticos, imagen, sociales, clientes, culturales, legales, proveedores, comunidad local y sociedad.

Contexto Interno: Considera aspectos organizacionales como la estructura interna de la Organización, recursos humanos, filosofía y valores, políticas, misión, metas, objetivos y estrategias para lograrlos.

Control: Cualquier medida que tome la dirección u otros componentes de una organización gubernamental, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La planificación, organización y supervisión de las acciones suficientes para proporcionar una seguridad razonable de que se alcancen los objetivos y metas, corresponde al jefe superior.

Control Interno: Proceso efectuado por todo el personal de una organización gubernamental, para proporcionar un grado de seguridad razonable en cuanto al logro de los objetivos dentro de las siguientes categorías: a) Eficacia y eficiencia de las operaciones, b) Fiabilidad de la información, y c) Cumplimiento de las leyes y normas aplicables.

Dentro del marco integrado se identifican cinco elementos de control interno que se relacionan entre sí y son inherentes al estilo de gestión de la empresa. Estos son:

- Entorno de Control.
- Evaluación de Riesgos.
- Actividades de Control.
- Información y Comunicación.
- Actividades de Supervisión.

Controles Claves Existentes: Todas las medidas claves que toma la organización con la finalidad de evitar la ocurrencia de un riesgo potencial, es decir, mitigar la ocurrencia del riesgo y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La organización planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas.

Control de Riesgos: La parte del Proceso de Gestión del Riesgo que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar riesgos advertidos.

Coordinación: Corresponderá que la política de Gestión de Riesgos vincule y coordine con otros procesos de la Institución, tales como Auditoría Interna y Control, Jurídico y Fiscalía, entre otros. Esto, por ejemplo, ante la existencia de Informes de Contraloría General de la República (CGR) y/o Hallazgos de Auditoría Interna, entre otros, donde sea necesaria una retroalimentación al Sistema.

Corto Plazo: La planificación o el horizonte de tiempo que trata con eventos del ciclo contable presupuestario, típicamente un año.

COSO: Un sistema de controles internos o estructura de controles definidos por el Comité de Organizaciones Patrocinadores de la Comisión Treadway (USA).

Criterio Profesional: Criterio o juicio basado en experiencia y conocimientos de las personas en la resolución de problemas y toma de decisiones. De acuerdo con el Marco Integrado de Control Interno, el Marco requiere la aplicación del criterio profesional a la hora de diseñar, implementar y ejecutar el sistema de control interno y evaluar su eficacia.

Criterios de Riesgo: Principios u otras reglas de decisión mediante las cuales se evalúa la importancia de los riesgos para determinar si se recomiendan acciones de tratamiento para ellos. Los criterios de riesgo pueden incluir costos y beneficios asociados, requerimientos legales y estatutarios, aspectos socioeconómicos y ambientales, las preocupaciones de los interesados, prioridades y otros aspectos para la evaluación.

Críticidad: Característica que se fundamenta entre otras variables, en el nivel del riesgo y en su importancia estratégica.

Cumplimiento: Conformidad y adhesión a las políticas, planes, procedimientos, leyes, regulaciones, contratos y otros requerimientos.

D

Deber de abstención: El Personal deberá abstenerse de las votaciones y/o decisiones en razón de su cargo, que signifiquen la influencia, en favor o en contra, al existir conflictos de intereses. En caso de contar con uno o más motivos de abstención el Personal deberá dejar manifiesta dicha situación por escrito, comunicándole a su jefatura directa conforme al Instructivo de Prevención de Conflictos de Interés. Cabe indicar que la no abstención en los casos en que proceda dará lugar a responsabilidad administrativa. Son motivos de abstención los contemplados en el artículo N°12 de la Ley N°19.880, sobre Bases de los Procedimientos Administrativos de los Órganos de la Administración del Estado.

Deficiencia de Control Interno: De acuerdo con el Marco Integrado de Control Interno, se refiere a un fallo relativo a uno o varios componentes y principios relevantes que podrían reducir la probabilidad de que una organización alcance sus objetivos.

Deficiencia de Control Interno Grave: De acuerdo con el Marco Integrado de Control Interno, se refiere a uno o múltiples fallos de control interno que reducen significativamente la probabilidad de que una entidad alcance sus objetivos y que por tanto no se pueda concluir que uno o más principios o componentes estén presentes y en funcionamiento. Una deficiencia de control interno o una combinación de deficiencias que reduzcan de forma severa la probabilidad de que una organización consiga lograr sus objetivos se denomina una Deficiencia Grave.

De Forma Integrada: Concepto utilizado en el Marco Integrado de Control Interno. Se refiere a la determinación de que los cinco componentes reducen colectivamente, a un nivel aceptable, el riesgo de no alcanzar un objetivo. Los componentes no deben ser considerados por separado, sino que han de funcionar juntos como un sistema integrado.

Delitos Funcionarios (DF): 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, es decir, por todo aquel que desempeñe un cargo o función pública.

Desagregación de Procesos: Identificación de unidades organizacionales componentes en un proceso. Por ejemplo, en subprocesos relevantes. A nivel de subproceso en etapas relevantes, etc.

Descripción del Riesgo: Identificación detallada de la situación o hecho que podría afectar el logro de los objetivos operativos de una etapa, subproceso o proceso.

Diagramas de Flujo de Datos o Flujogramas: Una representación gráfica de los flujos de información y cómo estos flujos se enlazan. Es una herramienta útil para Identificación de riesgos y para determinar los puntos de mayor exposición.

Diccionario de Riesgos: Compilación de definiciones generales relacionadas al proceso de gestión de riesgos, para asegurar un lenguaje común dentro de un sector.

Dueño del Riesgo: Quien tiene la responsabilidad y autoridad para gestionar un riesgo.

E

Eficacia: Grado de cumplimiento de los objetivos planteados en la organización gubernamental, sin considerar necesariamente los recursos asignados para ello. La calidad del servicio es una dimensión específica del concepto de eficacia que se refiere a la capacidad de la organización gubernamental para responder en forma rápida y directa a las necesidades de sus clientes, usuarios o beneficiarios.

Eficiencia: Relación entre dos magnitudes: la producción de un bien o servicio y los insumos o recursos que se utilizaron para alcanzar aquellos. Se refiere a la ejecución de las acciones, beneficios o prestaciones del servicio utilizando el mínimo de recursos posibles.

Efectividad del Sistema de Control Interno: El Marco Integrado de Control Interno, establece los requisitos de un sistema de control interno efectivo, el cual proporciona una seguridad razonable respecto a la consecución de los objetivos de la organización gubernamental. Así como reduce, a un nivel aceptable, el riesgo de no alcanzar un objetivo de la organización gubernamental y puede hacer referencia a una, a dos, o a las tres categorías de objetivos. Para ello, es necesario que se cumplan dos requisitos: Que cada uno de los cinco componentes y principios relevantes estén presente y en funcionamiento. Y que los cinco componentes funcionen “de forma integrada”. Cuando exista una deficiencia grave respecto a la presencia y funcionamiento de un componente o principio relevante, o con respecto al funcionamiento conjunto e integrado de los componentes, la organización gubernamental no podrá concluir que ha cumplido los requisitos de un sistema de control interno efectivo.

Ejecución de la Auditoría: Realización de las actividades programadas, en base a procedimientos y técnicas específicas, con el objetivo de determinar el nivel de exposición al riesgo en el proceso auditado.

Eliminación de Riesgos: Supresión de todos los riesgos asociados al desarrollo de un proceso o actividad. En la práctica no es posible hacer que desaparezcan todos los riesgos, ya que existen riesgos inherentes al desempeño de las actividades.

Encargado de Riesgos: El administrador o ejecutivo quién reporta al Jefe de Servicio y su equipo directivo la exposición de riesgos de la organización y las acciones alternativas de la misma, necesitadas para aliviarlos.

En Funcionamiento: Concepto utilizado en el Marco Integrado de Control Interno. Se refiere a la determinación de que los componentes y principios relevantes están siendo aplicados en el sistema de control interno para alcanzar los objetivos especificados.

Entorno/Ambiente de Control: Componente del Marco Integrado de Control Interno, el entorno de control es el conjunto de normas, procesos y estructuras que constituyen la base sobre la que desarrollar el control interno de la organización gubernamental. El Jefe de Servicio y su equipo directivo son quienes establecen el "Tone at the top" o “Tono desde la Dirección” con respecto a la importancia del control interno y las normas de conducta esperables. Elemento fundamental del sistema de control interno. Se refiere a la actitud y acciones de la dirección respecto a la importancia del control dentro de la organización. El entorno de control proporciona disciplina y estructura para la consecución de los objetivos principales del sistema de control interno. El entorno de control contiene elementos como; integridad y valores éticos; filosofía de dirección y estilo de gestión; estructura de la organización; asignación de autoridad y responsabilidad; políticas y prácticas de recursos humanos y compromiso de competencia profesional.

Ética: Es el conjunto de principios, valores, costumbres y normas que rigen la conducta humana.

Establecimiento de Roles y Responsables: Definición documentada y aprobada de los roles y responsabilidades de las personas relacionadas con las materias relativas al Proceso

de Gestión de Riesgos, como la prevención de efectos de los riesgos, el control del tratamiento de los riesgos, la identificación de problemas relativos a la gestión de los riesgos, la recomendación de soluciones y el monitoreo entre otras.

Estatuto de Auditoría Interna: Documento formal que define el objetivo, autoridad y responsabilidad de la actividad de auditoría interna, El estatuto debe: (a) establecer la posición de la actividad de auditoría interna dentro de la organización; (b) autorizar el acceso a los registros, al personal y a los bienes pertinentes para la ejecución de los trabajos; y(c) definir el ámbito de actuación de las actividades de auditoría interna.

Estrategias: Tácticas globales que permiten enfrentar la problemática de gestionar los riesgos, desde el punto de vista de su nivel de severidad y del nivel de la exposición al riesgo. Existen cuatro estrategias globales: aceptar, reducir, compartir y evitar.

Etaa Relevante: Componente estratégico de carácter relevante en un subproceso o proceso compuesto por actividades o tareas.

Evaluación del Riesgo: Dentro del Proceso de Gestión de Riesgos, la evaluación del riesgo es el proceso global de identificación del riesgo, de análisis del riesgo y de valoración del riesgo. Así mismo, como componente del Marco Integrado de Control Interno, 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.

Evento: Hecho imprevisto, o que puede suceder. Un incidente o situación, la cual ocurre en un lugar particular durante un intervalo de tiempo particular. El evento puede ser cierto o incierto. El evento puede ser una ocurrencia única o una serie de ocurrencias.

Evidencia de Auditoría: La evidencia de auditoría es la información que obtiene el auditor para extraer conclusiones en las cuales sustenta su opinión y está constituida por todos aquellos hechos susceptibles de ser probados por el auditor en relación con la materia que examina, que se le manifiesta a través de las técnicas de auditoría aplicada y de acuerdo con el juicio profesional.

Evidencia Electrónica de Auditoría: Se define como cualquier información creada, transmitida, procesada, grabada o mantenida electrónicamente que el auditor utiliza para respaldar el contenido de un informe de auditoría.

Evitar un Riesgo: Corresponde a una estrategia global para el proceso de gestión de riesgos que consiste en salir de las actividades que generen los riesgos.

Exposición al Riesgo: El riesgo que permanece después de que la dirección haya realizado sus acciones para reducir el impacto y/o la probabilidad de un acontecimiento adverso, incluyendo las actividades de control en respuesta a un riesgo.

Exposición al Riesgo Ponderado: Corresponde al nivel de exposición al riesgo multiplicado por el nivel de importancia o relevancia estratégica del proceso en el servicio. (Ver justificación de la ponderación).

F

Factores de Riesgo: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición.

Fase de Análisis de Riesgos: Paso del proceso de gestión de riesgos que consiste en el examen de los riesgos en relación a su severidad (probabilidad y consecuencia), efectividad de los controles y la exposición al riesgo.

Fase de Comunicación y Consulta: Paso del proceso de gestión de riesgos que consiste en comunicar, informar y consultar a los interesados internos y externos, según resulte

apropiado en cada etapa del proceso de gestión de riesgos, interpretando un proceso como un todo.

Fase de Evaluación de Riesgos: Paso del proceso de gestión de riesgos que consiste en comparar el riesgo estimado contra criterios predeterminados, niveles de riesgo deseable u otros criterios, estableciendo un ranking de priorización.

Fase de Valoración de Riesgos: Paso del Proceso de Gestión de Riesgos que consiste en comparar el riesgo estimado contra criterios predeterminados, niveles de riesgo deseables u otros criterios, estableciendo un ranking de priorización.

Fase Establecer el Contexto: Paso del proceso de gestión de riesgos que contempla la definición del entorno interno y externo de la entidad, además de la definición de la estructura de análisis y alcance del proceso de gestión de riesgos, denominado entorno o contexto de gestión de riesgo.

Fase Identificación de Riesgos y Oportunidades: Fase del proceso de gestión de riesgos que considera la identificación de riesgos y oportunidades que pueden afectar la consecución de los objetivos estratégicos de la entidad. Las oportunidades y riesgos, son eventos, que se definen como un incidente que emana de fuentes internas o externas que afecta positiva o negativamente la implementación de la estrategia o logro de los objetivos.

Fase Monitorear y Supervisar: Paso del proceso de gestión de riesgos en el cual se definen y utilizan mecanismos para monitorear y revisar el desempeño del proceso de gestión de riesgos y dar cuenta de la evolución del nivel del riesgo en proceso críticos para la administración.

Fase Tratamiento de Riesgos: Paso del proceso de gestión de riesgos que corresponde a la selección e implementación de opciones apropiadas para manejar el riesgo. Las medidas de tratamiento de los riesgos pueden incluir evitar, reducir, compartir o aceptar el riesgo.

Financiamiento del Terrorismo (FT): La Ley N°18.314 que Determina Conductas Terroristas y Fija su Penalidad, en su artículo 8 se refiere al delito de financiamiento del terrorismo, señalando que: “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”.

Formación: Tendrá como propósito llevar a cabo iniciativas para desarrollar y fortalecer el comportamiento íntegro del personal de la Institución. Estará compuesta por, al menos:

- **Campañas de Difusión:** Acciones periódicas que permitan socializar y comunicar el objetivo y principales herramientas de la Política de Gestión de Riesgos.
- **Capacitaciones:** Actividades de formación cuyo objetivo principal será perfeccionar los conocimientos, habilidades y actitudes del personal, para que puedan ajustar su desempeño a los estándares éticos institucionales esperados, incluyendo la etapa de inducción de los nuevos funcionarios del GORE RM.

Frecuencia: Una medida de incidencia, expresada en el número de incidentes de un evento en un plazo determinado. Probabilidad o ratio de ocurrencia de un evento expresado como el número de ocurrencias de un evento dado en el tiempo.

Fuente de riesgos: Se refiere al origen que pueden tener los riesgos. Existen riesgos de fuente externa, que son aquellos que nacen de situaciones que están fuera de la administración y control de la institución y riesgos de fuente interna son aquellos originados dentro del servicio, como los relacionados a las capacidades del personal y a la efectividad de los sistemas de información.

G

Gestión de Riesgos: Es un proceso estructurado, consistente y continuo implementado a través de toda la organización gubernamental para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el logro de sus objetivos.

Gobernanza: Combinación de sistemas, procesos y estructuras organizativos implantados por el jefe superior para informar, dirigir, gestionar y vigilar las actividades de la organización gubernamental, con el fin de lograr sus objetivos.

Gobierno Corporativo (Corporate Governance): La reacción estratégica de la organización a los riesgos. Generalmente incluye varias actividades y funciones, como dirección, seguridad, administración, estructura, etc. El ejercicio del poder es efectuado por medio del equipo de gobernanza constituido por la alta gerencia y la junta directiva.

Gobierno Electrónico: Corresponde al uso de tecnologías de información y comunicación (TIC) para mejorar y simplificar los servicios e información ofrecidos por el Estado a los ciudadanos, mejorar y simplificar los procesos de soporte institucional y facilitar la creación de canales tecnológicos que permitan aumentar la transparencia y participación ciudadana.

H

Horizontes de Tiempo: Perspectivas de planificación usados en la gestión de riesgo y planificación estratégica para representar distintos periodos de tiempo: corto plazo, mediano plazo y largo plazo.

I

Impacto: Consecuencia que puede ocasionar a la organización la materialización del riesgo. Puede haber más de una consecuencia de un mismo evento. Las consecuencias pueden estar en el rango de positivas a negativas. Las consecuencias se pueden expresar cualitativa o cuantitativamente. Las consecuencias se determinan en relación con el logro de objetivos.

Imparcialidad: Objetividad, carencia de prejuicios en favor o en contra de alguien o algo, que permite juzgar o proceder con rectitud.

Información Reservada: Documentos, datos o informaciones que no pueden ser proporcionados a terceros de conformidad a lo establecido en el artículo 21 de la Ley 20.285, sobre Acceso a la Información Pública.

Incertidumbre: Una condición donde el resultado sólo puede ser estimado y no medido.

Independencia: libertad de condicionamientos que amenazan la objetividad o la apariencia de objetividad. Tales amenazas deben ser vigiladas para asegurar que se mantenga la objetividad a nivel del auditor individual, trabajo, función y organización.

Informe de Auditoría: Es el resultado de la información, estudios, investigaciones y análisis efectuados por los auditores durante la realización de una auditoría, que, en una forma normalizada, expresa por escrito su opinión sobre el área o actividad auditada en relación con los objetivos fijados, señala las debilidades de control y formula recomendaciones pertinentes para eliminar las causas o deficiencias y establecer las medidas correctivas adecuadas.

Información y Comunicación: Componente del Marco Integrado de Control Interno. La información es necesaria para que la organización gubernamental pueda llevar a cabo sus responsabilidades de control interno y soportar el logro de sus objetivos. El Jefe de Servicio necesita información relevante y de calidad, tanto de fuentes internas como externas, para apoyar el funcionamiento de los otros componentes del control interno. La comunicación es el proceso continuo e iterativo de proporcionar, compartir y obtener la información necesaria.

Integridad: Conjunto de valores éticos y aspectos legales que orientan el correcto e imparcial comportamiento de los funcionarios/as, así como de todo miembro del personal de la Institución, contribuyendo a la lucha contra la corrupción y al fortalecimiento de la confianza pública, en pos de la Administración Superior de la Región.

Interés Particular: También llamado interés personal, está asociado a cualquier beneficio que pueda percibir el Personal del Gobierno de Santiago, o cualquier persona vinculada a esta (por relaciones de parentesco, afectividad, propiedad, gestión y/o negocios), de manera directa o indirecta.

J

Justificación de la Ponderación: Argumentos que fundamentan la importancia o relevancia que les da la dirección a los procesos del Servicio y a los subprocesos al interior de los procesos. La justificación debe estar basada en variables asociadas al nivel de contribución del proceso a la misión y objetivos estratégicos, el impacto en la imagen institucional, los recursos involucrados y la cobertura, entre otras consideraciones. (Ver ponderación estratégica y exposición al riesgo ponderado).

L

Largo Plazo: La planificación u horizonte de tiempo que trata con eventos más allá del corto plazo y mediano plazo, típicamente mayor a tres años.

Lavado de Activos (LA): Busca ocultar o disimular la naturaleza, origen, ubicación, propiedad o control de dinero y/o bienes obtenidos ilegalmente. Implica introducir en la economía activos de procedencia ilícita, dándoles apariencia de legalidad al valerse de actividades lícitas, lo que permite a delinquentes y organizaciones criminales disfrazar el origen ilegal de su producto, sin poner en peligro su fuente

Levantamiento de Procesos: El levantamiento de procesos constituye la forma de describir la realidad de la manera más exacta posible. El objetivo es hacer tangible el accionar de la organización para facilitar la definición de estándares internos que favorecen las instancias de mejoras. Los objetivos fundamentales en cada organización deben enfocarse en contar con todos los procesos documentados, actualizados y concordantes con el quehacer habitual.

Lluvia de Ideas: Una herramienta útil para la evaluación de riesgos, que intenta aprovechar y estimular una producción de ideas de un grupo de trabajo.

M

Marco de Trabajo de la Gestión del Riesgo: Conjunto de elementos que proporcionan los fundamentos y las disposiciones de la organización para el diseño, la implantación, el monitoreo, la revisión y la mejora continua de la gestión del riesgo en toda la organización.

Matriz de Riesgos Estratégica: Una herramienta usada para dar sistematizar el análisis de los procesos, sus riesgos, la severidad de los mismos, los controles asociados y la exposición al riesgo que presenta cada uno.

Medición de Riesgos: La evaluación del nivel de criticidad de los riesgos.

Mediano Plazo: El horizonte de tiempo que trata de los eventos entre corto plazo y largo plazo.

Metas: Objetivos medibles de planes o de acciones definidas por la dirección.

Mitigación de Riesgos: Acciones desarrolladas que tienen como resultado la disminución de los riesgos.

Modelamiento de los Controles: Se trata de un proceso que consiste primero en la

identificación de los controles asociados a los riesgos y posteriormente en su clasificación y calificación, de acuerdo a su nivel de cumplimiento con las normas de control interno y según su oportunidad, periodicidad y automatización.

Modelamiento de los Riesgos: Se trata de un proceso que consiste primero en la identificación de aquellas situaciones cuya ocurrencia u omisión pudieran afectar total o parcialmente el logro de los objetivos operativos. Otro paso corresponde a la calificación de la fuente y tipología del riesgo y por último a la calificación de la severidad del riesgo en términos de probabilidad e impacto.

Modelos: Diseños o esquemas que describen, explican o ayudan a la mejor comprensión y aplicación práctica de conceptos sobre gestión de riesgos, control interno o auditoría interna.

Monitorear: Verificar, supervisar, observar críticamente o medir el progreso de una actividad, acción o sistema en forma regular para identificar cambios respecto del nivel de desempeño requerido o esperado.

N

Nivel de Exposición al Riesgo: Es la medida de riesgo residual que se mantiene después de aplicados los controles existentes.

Nivel de Riesgo: Severidad ante la ocurrencia del riesgo. Se determina por la relación $\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$.

Norma (Standard): Una serie de criterios o requisitos que son aceptados generalmente por organismos competentes.

Normas Específicas de Control: Son los mecanismos o procedimientos que permiten alcanzar los objetivos de control. Estas normas comprenden las políticas específicas, los procedimientos, los planes de la organización.

O

Objetividad: Es una actitud mental independiente, que exige que los auditores internos lleven a cabo sus trabajos con honesta confianza en el producto de su labor y sin comprometer de manera significativa su calidad. La objetividad requiere que los auditores internos no subordinen su juicio al de otros sobre temas de auditoría.

Objetivo de la Auditoría: Declaraciones establecidas por los auditores internos que definen los logros pretendidos del trabajo.

Objetivos Operativos: Finalidad principal de gestión que se debe alcanzar en una etapa componente de un subproceso o proceso de una organización.

Objetivos Estratégicos de la Organización: Aquellos objetivos definidos y presentados en la Definición Estratégica a la Dirección de Presupuestos.

Obstáculos: Factores negativos que impiden alcanzar los objetivos.

Oportunidad: Un evento incierto con un impacto o consecuencia positiva probable.

P

Parte Interesada: Persona u organización que puede afectar, ser afectada, o percibir que está afectada por una decisión o actividad de la Organización Gubernamental.

Percepción del Riesgo: Punto de vista de una parte interesada sobre un riesgo.

Papeles de Trabajo: Los documentos (físicos y electrónicos) que respaldan el trabajo, que son preparados y guardados por los auditores. Estos papeles deben registrar la información obtenida y los análisis efectuados y servir de base para las observaciones y recomendaciones que se efectúen.

Perdida: Cualquier consecuencia negativa económica, financiera o de otro tipo.

Persistencia de un Riesgo: Hace referencia a la duración del impacto en la organización después de que el riesgo se haya materializado

Plan Anual de Auditoría: Plan que debe formularse anualmente y debe reflejar las metas para el año siguiente, los tipos de auditoría a realizarse, los procesos a auditarse, el alcance general de las auditorías, las estimaciones del uso de recurso, entre otros. El plan deberá ser anual y desarrollarse durante el periodo siguiente y su contenido debe emanar de análisis de riesgos realizado en la planificación.

Planes de Tratamiento y Monitoreo: Planes que define la dirección para gestionar los riesgos que se han priorizado en la fase evaluación de los riesgos y que deben señalar las estrategias y acciones orientadas a la gestión de riesgos.

Ponderación Estratégica: Nivel de importancia de cada proceso (en porcentaje), de acuerdo a su relevancia en la consecución de la misión y objetivos estratégicos del servicio y a cada subproceso dentro de un proceso, en relación a su nivel de importancia en el logro de los objetivos del mismo. (Ver justificación de la ponderación).

Política de Riesgos: Documento formal aprobado por la dirección que debe definir y documentar la disposición y actitud de la entidad ante el riesgo, conteniendo a lo menos los objetivos y compromisos con la gestión de riesgo, el alineamiento entre la política y los objetivos estratégicos, el alcance o amplitud de la política, los responsables de gestionar los riesgos y las competencias que éstos requieren, el compromiso de la dirección para la revisión periódica.

Presente: Concepto utilizado en el Marco Integrado de Control Interno. Se refiere a la determinación de que los componentes y principios relevantes existen en el diseño e implementación del sistema de control interno para alcanzar los objetivos especificados.

Principio de Probidad: Consiste en observar una conducta funcionaria intachable, un desempeño honesto y leal de la función a cargo, con preeminencia del interés general sobre el particular.

Principios del Marco Integrado de Control Interno: Son los principios que representan los conceptos fundamentales asociados a cada componente del Marco. Dado que proceden directamente de los componentes, la organización gubernamental 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, así como también a los objetivos individuales dentro de las categorías.

Probabilidad: La posibilidad de ocurrencia de un resultado o riesgo específico. La probabilidad se puede expresar en términos cuantitativos, mediante escalas que identifiquen niveles desde muy improbables hasta casi certeza.

Procedimiento Disciplinario: Conjunto de actividades destinadas a investigar determinadas conductas de los funcionarios o funcionarias, que pudieran constituir incumplimiento de sus deberes o transgresión de prohibiciones, susceptibles de ser sancionados con una medida disciplinaria. Tiene por objeto verificar la existencia efectiva de dichos hechos, la individualización de los responsables y su participación y aplicar las sanciones correspondientes, si procediere. Son procedimientos disciplinarios la Investigación sumaria y el sumario administrativo, aplicándose este último cuando la naturaleza de los hechos denunciados o su gravedad así lo exigieren.

Proceso: Conjunto de actividades íntimamente relacionadas que existen para generar un bien o un servicio, que cuentan con un ingreso de recursos, una transformación de éstos y una salida de servicios o productos, que tienen un cliente interno o externo a la organización.

Proceso Crítico: Aquellos procesos identificados como claves para el logro de la misión institucional a través del cumplimiento de los objetivos estratégicos.

Proceso de Apoyo o de Soporte: Procesos que apoyan administrativamente al resto de los procesos de la Organización. Sus “clientes” son internos. Ejemplos: Selección de personal, Formación del personal, Compras, Sistemas de información.

Proceso de Gestión del Riesgo: 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 identificación y manejo de éstos recae sobre la dirección.

Procesos de Control: Políticas, procedimientos y actividades, los cuales forman parte de un enfoque de control, diseñados para asegurar que los riesgos estén contenidos dentro de las tolerancias establecidas por el proceso de evaluación de riesgos.

Proceso Estratégico: Procesos que soportan la estrategia institucional. Son procesos destinados a definir y controlar las metas de la organización, sus políticas y estrategias. Permiten llevar adelante la organización. Están en directa relación con la misión/visión de la organización. Involucran personal de primer nivel de la Organización Gubernamental.

Proceso de Negocio: Procesos directamente relacionados con los productos y servicios entregados por las organizaciones gubernamentales a los ciudadanos, por lo que inciden directamente en la satisfacción final de los mismos. Generalmente involucran varias áreas o departamentos.

Procesos Transversales en la Administración del Estado: Corresponde a una denominación que considera todos aquellos procesos que cuentan con características organizacionales comunes en la Administración del Estado.

Procedimientos de Auditoría: Se definen como las herramientas utilizadas por los auditores para obtener la evidencia necesaria, con el propósito de formarse un juicio profesional sobre las actividades examinadas y determinar fundadamente el nivel de exposición al riesgo del proceso o riesgos analizados.

Puntos de Interés del Marco Integrado de Control Interno: Representan características relacionadas con el principio. Cada principio es apoyado por atributos, que se denominan “puntos de interés”. Generalmente se espera que cada atributo esté presente en el principio y puede ser posible tener un principio presente y funcionando sin tener todos los puntos de interés.

R

Ranking de Riesgos: Ordenamiento de procesos, subprocesos, etapas o riesgos de acuerdo a criterios preestablecidos.

Reducción de Riesgos: Una de las estrategias globales para tratar los riesgos de una entidad, que consiste en una aplicación selectiva de las técnicas apropiadas y principios administrativos para reducir la posibilidad de una ocurrencia o sus consecuencias, o ambas.

Retroalimentación: En sistemas y modelos, el flujo de información sobre la condición actual de variables desde su origen o hasta la fuente con el propósito de observar el avance de los objetivos establecidos.

Registro del Riesgo: Registro de la información relativa a los riesgos identificados.

Reporte del Riesgo: Forma de comunicación destinada a informar a determinadas partes interesadas, internas o externas, proporcionándoles información del estado actual del riesgo y de su gestión.

Riesgo: Contingencia o proximidad de que suceda algo que tendrá un impacto en los objetivos. La posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

Riesgo Aceptado: Ver apetito de riesgo.

Riesgo Asociado: Cualquier situación relevante que entorpece el normal desarrollo e impide el logro de un objetivo. El riesgo se mide en términos de consecuencias y probabilidad. (Ver riesgo y riesgo relevante).

Riesgo de Auditoría: representa la posibilidad de que el auditor exprese una opinión errada en su informe debido a que la información suministrada a él esté afectada por una distorsión material. El auditor debe evaluar el nivel de riesgo existente en un trabajo específico y tener presente que debe arbitrar todos los medios a su alcance para reducir el riesgo a niveles técnicamente aceptables $ra = rd + rc$.

Riesgo de Cartera: Es el riesgo de que una combinación de proyectos, activos, unidades o lo que exista en la cartera no alcanzará para lograr los objetivos totales de la cartera debido a una mala balanza de riesgos dentro de la cartera.

Riesgo de Control: Es la posibilidad de que los procedimientos de control interno incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores significativos de manera oportuna. Este riesgo si bien no afecta a la entidad como un todo, incide de manera directa en los componentes.

Riesgo de Detección: Se origina al aplicar procedimientos que no son suficientes para lograr descubrir errores o irregularidades que sean significativos, es decir, que no detecten una debilidad de control hallazgo que pudiera ser importante.

Riesgo Específico: Son los riesgos operativos que pueden afectar los objetivos de una Etapa o Subproceso, entendiendo como tales, aquellas situaciones cuya ocurrencia u omisión pudieran afectar total o parcialmente el logro de sus objetivos operativos.

Riesgos Inherentes: Es la posibilidad de que existan errores o irregularidades en la gestión administrativa y financiera, antes de verificar la eficiencia del control interno diseñado y aplicado por el ente a ser auditado. Este riesgo tiene relación directa con el contexto global de una institución e incluso puede afectar a su gestión.

Riesgo Residual: El nivel de riesgo restante luego del tratamiento del riesgo. El nivel remanente del riesgo después de que se han tomado medidas de tratamiento del riesgo. (Ver exposición al riesgo).

Riesgo Relevante: (ver riesgo asociado).

Roles y responsables: (Ver establecimiento de roles y responsables).

S

Servicios de Aseguramiento: Un examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización.

Severidad del Riesgo: Corresponde al nivel del riesgo originado por la relación entre la consecuencia y la probabilidad de ocurrencia. (Ver nivel de riesgo).

Sistema de Integridad: Es el conjunto de normas, procedimientos, herramientas e iniciativas destinadas a promover y reforzar la integridad de cada uno de los funcionarios y

funcionarias del GORE RM, permitiendo disminuir los riesgos de corrupción en todos los niveles y procesos de la Institución.

Subproceso: Corresponden a aquellos componentes principales en la estructura de un proceso de gestión o soporte.

T

Taxonomía Matriz de Riesgos (XBRL): Es un diccionario de conceptos y relaciones construido bajo el estándar XBRL – “Extensible Business Reporting Language”, creado por el Consejo de Auditoría Interna General de Gobierno.

Tipología de Riesgos: Es una clasificación en tipos de riesgos generales, que incluye categorías de riesgos de fuente interna y externa.

Tolerancia al riesgo: Es el nivel aceptable de la variación alrededor del logro de un objetivo de negocio específico y se debe alinear con el apetito del riesgo de una organización.