PROGRAMA MARCO

CONSEJO
DE AUDITORIA
INTERNA
GENERAL
DE GOBIERNO

OBJETIVO DE AUDITORÍA GUBERNAMENTAL 2009 y PRIMER TRIMESTRE 2010 - Nº 3

DOCUMENTO TÉCNICO
Nº 41

MARZO 2009

TABLA DE CONTENIDOS

I.- INTRODUCCIÓN

Para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 - Nº 3 del año, se pretende continuar optimizando el levantamiento de procesos realizado, mejorar la identificación y descripción de los objetivos, riesgos y controles y, en especial, la formulación de las medidas de tratamiento de los riesgos. Adicionalmente, las jefaturas del Servicio deben incluir, en la Matriz de Riesgos Estratégica, los procesos sistemas o programas que se han creado o reformulado durante el año 2009.

El rol principal de la auditoría interna en este proceso ha sido coordinar las actividades para introducir el Proceso de Gestión de Riesgos. Para este año 2009, nuevamente, la Auditoría Interna debe proveer aseguramiento a la dirección sobre la efectividad de la gestión de los riesgos mediante el cumplimiento del Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 - Nº 2, cuyos resultados en conjunto con las directrices emitidas por el Consejo de Auditoría Interna de Gobierno, servirán para retroalimentar el proceso y actualizar la política, matriz de riesgos, ponderaciones, ranking de procesos y planes de tratamiento, entre otros elementos.

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

Como punto I esta introducción; en el punto II se señala el objetivo general del documento; en el punto III, su relación con el Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 – Nº 2; en el punto IV el marco metodológico para la actualización del Proceso de Gestión de Riesgos para el año 2009; en el punto V, se establecen conceptos básicos del Proceso de Gestión de Riesgos; en el punto VI se señala el análisis de las fases del Proceso de Gestión de Riesgos en las entidades gubernamentales; en el punto VII se definen conceptos y elementos a incorporar para el Proceso de Gestión de Riesgos en las entidades del sector gubernamental bajo el Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 - Nº 3 y, en el punto VIII se señalan los requerimientos específicos para el Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 – Nº 3.

Finalmente, se adjuntan nueve anexos que contienen: en el Anexo Nº 1, un ejemplo de Política de Riesgos; en el anexo Nº 2 un ejemplo de asignación de roles y responsabilidades; en el anexo Nº 3 la descripción del rol del Auditor Interno en el Proceso de Gestión de Riesgos; en el anexo Nº 4 se entrega una guía para el levantamiento de procesos; el anexo Nº 5 establece las tablas de valuación para riesgos, controles y exposición; el anexo Nº 6 entrega un ejemplo de levantamiento de procesos; el anexo Nº 7 enuncia técnicas de identificación de eventos generados de riesgos y oportunidades; el anexo Nº 8 entrega un ejemplo de riesgos genéricos que afectan los procesos mejorados con Tecnologías de Información; el anexo Nº 9 define los conceptos generales de control; el anexo Nº 10 presenta un ejemplo de plan de tratamiento de riesgos con estrategias, acciones e indicadores y, por último en el anexo Nº 11 acompaña un ejemplo de Matriz de Riesgo Estratégica.

II.- OBJETIVO GENERAL DEL DOCUMENTO

Documentar los procedimientos que permitan a las entidades del Estado, cumplir satisfactoriamente con Objetivo Gubernamental 2009/Primer Trimestre 2010 - Nº 3 "Mantener y mejorar el Proceso de Gestión de Riesgos en las entidades de la Administración del Estado. Para ello, los Jefes de Servicio, deben dar cumplimiento a las directrices que sobre la materia formule el Consejo de Auditoría Interna General de Gobierno, lo que debe contemplar a lo menos los siguientes objetivos:

- Incorporar en el Proceso de Gestión de Riesgos, aquellos elementos que permitan avanzar hacia la consolidación del mismo y que serán oportunamente documentados por el Consejo de Auditoría Interna General de Gobierno;

- Generar mecanismos que permitan contar con información oportuna y confiable para el Proceso de Gestión de Riesgos, a lo menos semestralmente;

- Demostrar la debida implementación de las medidas preventivas y correctivas comprometidas para mejorar la gestión institucional y alcanzar los objetivos estratégicos del Servicio;

- Disponer los recursos necesarios para la correcta implementación y funcionamiento del Proceso de Gestión de Riesgos en la entidad;

- Asumir las autoridades superiores de los ministerios, servicios y empresas del Estado, la responsabilidad de la adopción de las medidas tendientes a la gestión efectiva de los riesgos, especialmente aquellos de mayor criticidad, informando de ello al Consejo de Auditoría Interna General de Gobierno".

III.- RELACIÓN CON OBJETIVO GUBERNAMENTAL 2009/PRIMER TRIMESTRE 2010 - Nº 2

Cómo se señaló precedentemente, durante el año 2008, las entidades del Sector Gubernamental siguieron con la mejora y revisión de sus Procesos de Gestión de Riesgos con la finalidad de conocer y administrar sus riesgos para perfeccionar el cumplimiento de sus objetivos estratégicos y operativos. A pesar del éxito que tuvo la revisión y mejora, existen elementos del Proceso de Gestión de Riesgos que presentan oportunidades de mejoras, los cuales se señalan en términos generales en el punto VIII del presente documento, que deben ser revisados y corregidos durante el año 2009.

El mejoramiento continuo del Proceso de Gestión de Riesgo, se logrará en base a la revisión y examen del proceso por parte del Servicio, identificando debilidades y estableciendo planes para superarlas. Para este análisis contará con el apoyo del correspondiente asesor de riesgos del Consejo de Auditoría.

Por otra parte, el Auditor Interno del Servicio, en cumplimiento del Objetivo Gubernamental 2009/2010 - Nº 2, deberá efectuar el aseguramiento al Proceso de Gestión de Riesgos, lo que se traduce en una auditoría de aseguramiento que deberá desarrollarse en base a los lineamientos técnicos que emanan del Documento Técnico Nº 42/2009, cuyos resultados deberán ser entregados al Jefe de Servicio y al Consejo de Auditoría, al 30 de junio del año 2009. Sobre los

resultados de esta auditoría y en base a su propia revisión, el Servicio deberá abocarse al mejoramiento del Proceso de Gestión de Riesgos. Además los resultados de todas las auditorías realizadas en el año, deberán ser considerados para el aseguramiento y mejora continua del Proceso de Gestión de Riesgos.

Es especialmente importante, la auditoría de aseguramiento que realice el Auditor Interno del Servicio, en base al Documento Técnico Nº 42, ya que de esta auditoría deberá emitirse un informe con hallazgos y sugerencias que se informarán al Consejo de Auditoría. Las sugerencias que emanen de ese informe de auditoría, serán obligatorias para el Servicio y deben ser implementadas para el mejoramiento del Proceso de Gestión de Riesgos. Para verificar el grado de implementación de dichas sugerencias, el auditor deberá realizar una auditoría de seguimiento, cuyos resultados también deben ser informados al Consejo de Auditoría.

En el caso que el Servicio no acepte alguna de las sugerencias del auditor, se entenderá que la dirección acepta este riesgo, haciéndose responsable de su potencial concreción y efectos.

La implementación de las sugerencias serán claves para el perfeccionamiento del Proceso de Gestión de Riesgos al interior del Servicio, que tendrá el plazo que se señala en este documento técnico para superar las debilidades observadas y contará con la asesoría del asesor de riesgos o sectorialista del Consejo de Auditoría.

IV.- MARCO METODOLÓGICO PARA LA ACTUALIZACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS PARA EL AÑO 2009

Este documento complementa algunos de los requerimientos contenidos en el Documento Técnico Nº 38/2008, y además entrega una visión integral del Proceso de Gestión de Riesgos, por lo que el presente documento se entenderá como el marco técnico para el Objetivo Gubernamental 2009/Primer Trimestre 2010 - Nº 3, y en general como documento marco para el funcionamiento y mantención del Proceso de Gestión de Riesgos.

V.- PROCESO DE GESTIÓN DE RIESGOS

1.- Algunos conceptos sobre Gestión de Riesgos

La Gestión de Riesgos es un proceso estructurado, consistente y continuo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos. Todos en la organización juegan un rol en el aseguramiento de éxito de la Gestión de Riesgos, pero la responsabilidad principal de la misma recae sobre la Dirección. [1]

La definición anterior se puede complementar con otros importantes elementos:

- La Gestión de Riesgos es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.
- Puede ser aplicada a todos los niveles de una organización, es decir, en los niveles estratégicos, tácticos y operacionales.

[1] Cfr. COSO II - ERM

- También puede ser aplicada a proyectos específicos, para sustentar decisiones específicas o para administrar áreas específicas de riesgo.
- Para cada fase del Proceso de Gestión de Riesgos deberían mantenerse registros adecuados, suficientes como para satisfacer a una auditoría externa o certificación independiente.
- No sólo considera la identificación y tratamiento de riesgos, sino que también las oportunidades que contribuyan al logro de los objetivos.
- La aplicación del marco teórico del Proceso de Gestión de Riesgos siempre debe adecuarse a la entidad y al sector que ésta pertenece.

Beneficios potenciales de la aplicación de la Gestión de Riesgos

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

2.- Modelos para la Gestión de Riesgos y de control interno

Si bien existe una diversidad de modelos para la gestión y evaluación de riesgos, en principio su concepto global es el mismo, con fundamentos financieros, matemáticos o analíticos quizá distintos. En este contexto, es necesario realizar un breve comentario sobre el modelo más utilizado en la actualidad, como es el de “Gestión de Riesgos Corporativos – Marco Integrado”, emitido por el Committee of Sponsoring of the Treadway Comisión (COSO), a finales del año 2004.

Este Marco también llamado COSO II fue definido por el referido Comité para ayudar a las organizaciones a gestionar los riesgos. Define el riesgo y la gestión de riesgos corporativos y proporciona definiciones básicas, conceptos, categorías de objetivos, componentes y principios de un marco integral de la gestión de riesgos corporativos. Su objetivo es proporcionar orientación a las organizaciones para determinar cómo mejorar dicha gestión, proporcionando el contexto y facilitando su aplicación en el mundo real. El Marco ha sido diseñado también para proveer una base para uso de las organizaciones en la tarea de determinar si su gestión de riesgos corporativos es eficaz y, en caso negativo, qué necesitan para que lo sea.

En comparación con el informe “Control interno – Marco Integrado”, emitido en el año 1992 por el Committee of Sponsoring of the Treadway Comisión (COSO), que estableció un marco para el control interno y proporcionó herramientas para que las organizaciones puedan evaluar sus sistemas de control, se observan las siguientes diferencias:

- El Marco Integrado de Control Interno está incluido en la gestión de riesgos corporativos y

forma parte de ella. Dicha gestión es más amplia que el control interno. La gestión de riesgos corporativos capacita a la dirección para identificar, evaluar y gestionar los riesgos en caso de incertidumbre, mejorando así la capacidad de generar valor. La gestión de riesgos corporativos incluye las siguientes capacidades: Alinear el riesgo aceptado y la estrategia, mejorar las decisiones de respuesta a los riesgos, reducir las sorpresas y pérdidas operativas, identificar y gestionar la diversidad de los riesgos para toda la organización, aprovechar las oportunidades y mejorar la dotación de capital.

- El Marco Integrado de Control Interno especifica tres categorías de objetivos: operaciones, información financiera y cumplimiento. Por su parte, el Marco Integrado de Gestión de Riesgos Corporativos, contiene también tres categorías similares: operaciones, información y cumplimiento. De éstas la categoría de información difiere de la estipulada en el Marco Integrado de Control Interno, en que incluye además de la información financiera de los estados financieros publicados, a todos los informes desarrollados por la organización, divulgados tanto interna como externamente, es decir, información no financiera.

- Adicionalmente, el Marco Integrado de Gestión de Riesgos Corporativos añade una categoría de objetivos denominada objetivos estratégicos, que operan a un nivel mayor que los otros y se derivan de la misión o visión de la organización.

- El Marco Integrado de Gestión de Riesgos Corporativos introduce los conceptos de riesgo aceptado y tolerancia al riesgo.

- El Marco Integrado de Gestión de Riesgos Corporativos, incorpora el concepto de “perspectiva de cartera de riesgos”. Este se refiere a que además de los riesgos considerados en el alcance de los objetivos de la organización a escala individual, es necesario tener en cuenta los riesgos compuestos desde una perspectiva de “cartera”. El Director responsable desarrolla una evaluación compuesta de ellos, y refleja su perfil de riesgo residual respecto de los objetivos y tolerancia al riesgo. Los riesgos individuales pueden ser tolerables, pero en su conjunto o desde una perspectiva de cartera, pueden superar el riesgo aceptado.

- El Marco Integrado de Gestión de Riesgos Corporativos amplía el componente de evaluación de riesgos del Marco Integrado de Control Interno, creando cuatro componentes - establecimientos de objetivos (que es un requisito previo para el control interno), identificación de eventos, evaluación de riesgos y respuesta al riesgo.

- El Marco Integrado de Gestión de Riesgos Corporativos amplía la necesidad establecida en el Marco Integrado de Control Interno de tener una misma masa crítica de miembros independientes en el consejo de administración, y establece que, para una gestión eficaz de riesgos corporativos, el consejo deberá tener al menos una mayoría de miembros externos e independientes.

- Los dos marcos en comparación reconocen que existen riesgos en cualquier nivel de la organización y que resultan de una variedad de factores internos y externos. Ambos marcos consideran la identificación de los riesgos en el contexto del impacto potencial sobre la consecución de los objetivos.

- El Marco Integrado de Gestión de Riesgos Corporativos plantea el concepto de eventos potenciales, definiendo un evento como un incidente o acontecimiento emanado de fuentes internas o externas que afecta a la implantación de la estrategia o al logro de los objetivos.

  Los eventos potenciales de impactos positivos representan oportunidades, mientras que los de impacto negativo representan riesgos. La gestión de riesgos corporativos implica identificar eventos potenciales y qué los provoca, utilizando una combinación de técnicas tradicionales con el uso de tendencias emergentes en su detección

- Aunque ambos marcos requieren una evaluación de riesgos en términos de probabilidad de que un determinado riesgo ocurra y de su impacto potencial, el Marco de Gestión de Riesgos Corporativos recomienda analizar los riesgos considerando que éstos son residuales o inherentes, preferiblemente expresados en la misma unidad de medida de los objetivos con que se asocian. Los horizontes temporales deben ser coherentes con las estrategias y objetivos de la organización y, cuando sea posible, con los datos observables. También se introduce el concepto de riesgos interrelacionados que describen cómo un solo evento puede crear múltiples riesgos.

- El Marco de Gestión de Riesgos Corporativos señala cuatro categorías de respuesta al riesgo: evitar, reducir, compartir y aceptar. Como parte de dicha gestión, la alta dirección considera las respuestas potenciales en estas categorías y las tiene en cuenta, con la intención de conseguir un nivel de riesgo residual en línea con las tolerancias al riesgo de la organización. Tras considerar las respuestas a los riesgos, individualmente o en grupo, la alta dirección contempla su efecto agregado en toda la organización.

- Ambos marcos presentan las actividades de control como una ayuda para asegurar que las respuestas al riesgo de la alta dirección se llevan a cabo. El Marco Integrado de Gestión de Riesgos Corporativos pone en relieve que, en algunos casos, las mismas actividades de control sirven de respuestas a los riesgos.

- El Marco Integrado de Gestión de Riesgos Corporativos amplía el componente de comunicación e información del control interno, destacando la consideración de datos derivados de eventos pasados y presentes, además de datos potenciales futuros.
  La existencia de un canal alternativo de comunicaciones, independiente a las líneas formales de información considerado en el Marco Integrado de Control Interno, tiene mayor énfasis en el Marco Integrado de Gestión de Riesgos Corporativos, que establece que esta gestión requiere de dicho canal para ser eficaz. Este canal alternativo se establece por la Dirección, cuando los canales habituales de información no resulten apropiados, su propósito es proporcionar un medio sencillo que permita a los funcionarios de una Institución comentar o informar de forma confidencial sobre un comportamiento real o percibido que pude ser ilegal, no ético o inadecuado. Se trata de canales que aseguren que se pueda comunicar un incidente sin riesgo de represalias.

- Ambos marcos centran la atención en los papeles y responsabilidades de algunas “partes organizativas” que forman parte del control interno y la gestión de riesgos corporativos o que les facilitan importante información. El Marco Integrado de Gestión de Riesgos Corporativos describe los roles y responsabilidades de los directores de riesgos y amplía el papel del consejo de administración de la organización.

Para mayor información sobre esta materia, el lector puede consultar www.coso.org.

3.- Fases Genéricas en el Proceso de Gestión de Riesgos

Sin perjuicio que en la actualidad existen una serie de modelos para la gestión de riesgos de mayor o menor difusión, como se señala al punto 2 anterior, el Consejo de Auditoría ha decidido utilizar un modelo genérico, que en su desarrollo y mejora a través del tiempo permita a las entidades gubernamentales adecuarlo a otros más específicos, si es que aquello fuese necesario.

Las fases en que se puede desagregar dicho modelo genérico se señalan a continuación:

- **Establecimiento del contexto:** Establecer los contextos estratégico, organizacional y de gestión en los cuales tendrá lugar el Proceso de Gestión de Riesgos. Deben establecerse los criterios contra los cuales se evaluarán los riesgos y definirse la estructura de análisis, los roles y responsabilidades.

- **Identificación de riesgos y oportunidades:** Identificar los riesgos que podrían impedir, degradar o demorar el cumplimiento de los objetivos estratégicos y operativos de la organización, así como las oportunidades que puedan contribuir al logro de los referidos objetivos.

- **Análisis de riesgos:** El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. Consecuencia y probabilidad se combinan para producir un nivel estimado de riesgo según la definición de la organización. Adicionalmente se debe identificar y analizar los controles mitigantes existentes.

- **Evaluación de riesgos:** Comparar los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

- **Tratamiento de riesgos:** De acuerdo al ranking de riesgos y al nivel de riesgo preestablecido por la organización (si es que ha sido establecido por la dirección), definir su tratamiento y/o monitoreo, desarrollando e implementando estrategias y planes de acción específicos, que mantengan el riesgo dentro de los niveles aceptados por la organización.

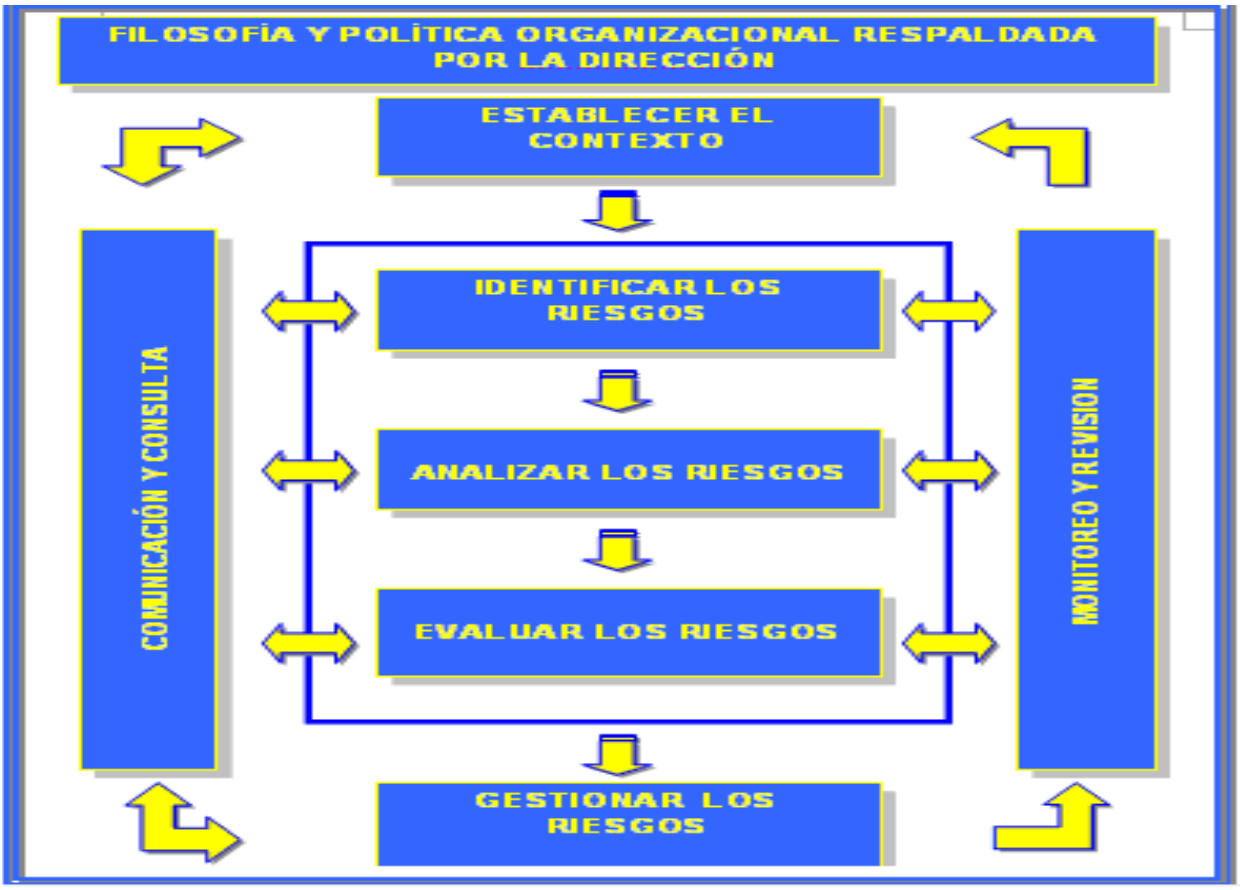
- **Monitoreo y revisión:** Definir y utilizar mecanismos para monitorear y revisar el desempeño del Proceso de Gestión de Riesgos y dar cuenta de la evolución del nivel del riesgo en procesos críticos para la administración.

- **Comunicación y consulta:** Definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos. Dichos mecanismos deben permitir a las autoridades tomar decisiones en forma oportuna respecto de los riesgos con mayores desviaciones en relación a los niveles aceptado.

En el cuadro Nº 1 se presenta un esquema representativo de la relación entre las fases genéricas que componen un Proceso de Gestión de Riesgos, bajo la perspectiva que se ha adoptado para la

implementación de este proceso y para el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3.

Cuadro Nº 1: Esquema representativo del Proceso de Gestión de Riesgos



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

- www.coso.org.
- www.erm.coso.org.
- NORMA IRAM 17750 - Sistema de Gestión de Riesgos.
- Estándar Australiano/Neozelandés AS/NZS 4360:1999.

VI.- ANÁLISIS DE LAS FASES DEL PROCESO DE GESTIÓN DE RIESGOS EN LAS ENTIDADES GUBERNAMENTALES

1.- Estado Actual

En consideración al desarrollo del Objetivo Gubernamental Nº 2 – 2007, y del Objetivo Gubernamental Nº 3 - 2008 y la naturaleza y características del Sector Gubernamental, se puede concluir que las entidades gubernamentales han implementado durante el año 2007 y mantenido y mejorado durante el año 2008, un Proceso de Gestión de Riesgos que ha permitido identificar los procesos críticos que afectan en distintos niveles a los objetivos estratégicos y, mediante la desagregación de dichos procesos, su ponderación en base a su relevancia para la entidad y el análisis de los riesgos y controles claves asociados a estos procesos, han construido la Matriz de Riesgo Estratégica, con el fin de determinar los eventos a ser tratados para mantener el riesgo del Servicio en un nivel aceptable, enunciando planes de tratamientos con acciones concretas para mitigar los riesgos.

Sin perjuicio del éxito que significó la señalada implantación del Proceso de Gestión de Riesgos en el año 2007 y su revisión y mejoramiento durante el año 2008, se han detectado algunas deficiencias y debilidades que se detallan en forma genérica en el punto VIII del presente documento, por lo cual es necesario avanzar en la calidad del proceso y en su mejora continua. En este camino, deben incorporarse con mayor fuerza las jefaturas superiores y todo el personal de las entidades del Estado, para propender a una mejora de la gestión de los riesgos. Para alcanzar este objetivo, se debe complementar el trabajo realizado durante el año 2008, revisando todo el proceso, superando las debilidades que se observen y profundizando el desarrollo de la gestión de riesgos.

Como se señaló anteriormente, el Proceso de Gestión de Riesgos consta de siete (7) fases. Para el año 2009, el contenido detallado de cada fase, y los elementos que serán solicitados en cada una de ellas, será tratado en los puntos VII y IX de este documento.

A continuación se señala el avance que ha tenido el Sector Gubernamental en cada fase del Proceso de Gestión de Riesgo durante el año anterior:

- **Fase Establecimiento del Contexto de la Gestión de Riesgos.** Se revisó la Política de Gestión de Riesgos, los responsables y sus roles, clasificaciones de procesos y ponderaciones estratégicas de los procesos, esta política y roles fueron revisadas para determinar si correspondían a la realidad del Servicio y fueron modificadas y mejoradas para hacer más eficiente y efectivo el Proceso de Gestión de Riesgos en la entidad.

  Se generó y actualizó un diccionario genérico o básico de riesgos por el Consejo de Auditoría con el fin de unificar el lenguaje que se utiliza, evitando generar incertidumbres y entendimientos distintos, frente a los conceptos relacionados con la gestión de riesgos, por parte de las personas que se desempeñan en la organización.

- **Fase Identificación de Riesgos**. Se clasificaron y actualizaron los riesgos en las diversas tipologías según lo instruido por el Consejo de Auditoría; se redefinieron y actualizaron algunos de los controles y se identificaron algunos riesgos del Sistema de Gobierno Electrónico.

- **Fase Análisis de Riesgos**. Se revisaron los riesgos, algunos se redefinieron y actualizaron y se valuaron de acuerdo a criterios de probabilidad e impacto y los controles mitigantes asociados, de acuerdo a su diseño y cumplimiento de normas de control.

- **Fase Evaluación de Riesgos.** Se formularon y en algunos casos se reformularon los ranking de riesgos ponderados de acuerdo a la importancia estratégica de los procesos y subprocesos para cada entidad.

  Destaca en las fases Análisis de Riesgos y Evaluación de Riesgos la utilización de la Aplicación CMM Control Matriz Management, que permitió en el año 2008 hacer una validación de la información contenida en la matriz de riesgos y su remisión en forma segura al Consejo de Auditoría.

- **Fase Tratamiento de Riesgos.** Se identificaron, revisaron y en algunos casos se redefinieron las estrategias para tratar los riesgos de acuerdo a su priorización. Pendiente queda su mejora e implementación para el presente año 2009.

- **Fase Monitoreo y Revisión.** Se establecieron estructuras para controlar la implementación de las estrategias para tratar los riesgos. En general, producto de la redefinición y reformulación de los Planes de Tratamiento de Riesgos durante el año 2008, queda pendiente la determinación del avance del tratamiento y sus efectos en los riesgos para el presente año 2009.

- **Fase Comunicación y Consultas.** Se revisaron y redefinieron diagnósticos de los procedimientos y sistemas para la comunicación del Proceso de Gestión de Riesgos en el Servicio (línea base) y se revisión y mejoró la propuesta para el periodo siguiente.

Como se señaló anteriormente, en la implementación del Proceso de Gestión de Riesgos en los Servicios se detectaron algunas deficiencias que deben ser mejoradas. Los insumos que deberán tenerse presente para el mejoramiento del Proceso de Gestión de Riesgos son fundamentalmente dos. En un primer lugar, la revisión que hace la propia administración que considere los cambios y ajustes producidos en la entidad. En un segundo lugar, la auditoría interna, tanto los resultados de la auditoría de aseguramiento del proceso, como los resultados de todas las auditorías que se realizan durante el año para el desarrollo normal de su plan anual de auditoría.

VII.- CONCEPTOS Y ELEMENTOS A INCORPORAR PARA EL PROCESO DE GESTIÓN DE RIESGOS EN LAS ENTIDADES DEL SECTOR GUBERNAMENTAL BAJO EL OBJETIVO GUBERNAMENTAL 2009/PRIMER TRIMESTRE 2010- Nº 3

En los párrafos siguientes, se revisará cada una de las fases del Proceso de Gestión de Riesgos, destacándose aquellos requerimientos que deben ser cumplidos por el Servicio para efectos del Objetivo Gubernamental 2009/Primer Trimestre 2010 - Nº 3.

1.- FASE ESTABLECIMIENTO DEL CONTEXTO

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

1.1.- Contexto interno y externo

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

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

En el Sector Gubernamental todos los Servicios han desarrollado esta fase, a través de la definición de su misión, objetivos y productos realizadas en base a las herramientas de gestión entregadas por la Dirección de Presupuestos en el Programa de Mejoramiento de la Gestión de Planificación y Control de Gestión, mediante el establecimiento de metas e indicadores y, naturalmente, a través de análisis que se realiza previo y durante la confección de la Matriz de Riesgo Estratégica. Ello significa que, en general, toda entidad ha identificado y analizado los elementos de su entorno interno y externo.

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

Establecer la política de riesgos. La política de riesgos se debe definir y documentar, aprobándose por la dirección y debe contener al menos los siguientes elementos:

- 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 procesos a ser utilizados para gestionar los riesgos.
- Los responsables de gestionar los riesgos y las competencias que estos requieren.
- El compromiso de la dirección para la revisión periódica.

La Dirección debe asegurar que la política de riesgos se incluya y sea coherente con la política de Calidad del Servicio, y, que sea publicada y comunicada a través de todos los niveles del Servicio, estableciendo responsables de las comunicaciones. En anexo Nº 1 se entrega un ejemplo de política de riesgos.

Durante el año 2007, los Servicios establecieron su política de gestión de riesgos que fue remitida al Consejo de Auditoría y que fue revisada, mejorada y en algunos casos reformulada en el marco del cumplimiento del Objetivo Gubernamental 2008 – Nº 3.

Acciones año 2009

Durante el año 2009, y en general, en forma permanente, la política de riesgos debe ser revisada para determinar su consistencia con las políticas y objetivos estratégicos del Servicio, poniendo especial énfasis en que la política de riesgos considere todos los procesos que ejecuta el Servicio y que sea consistente con la política de calidad del la entidad.

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

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

En anexo Nº 2, se presenta un ejemplo de asignación de roles y responsabilidades.

Es importante señalar que el Auditor Interno del Servicio no puede ser nombrado como responsable en estos temas, ya que se estaría afectando su objetividad e independencia al momento de auditar el funcionamiento y efectividad del Proceso de Gestión de Riesgos. En anexo Nº 3 se entrega un resumen del rol de la auditoría interna en un Proceso de Gestión de Riesgos, destacándose aquellas funciones que puede realizar y aquellas que no le están permitidas.

Acciones año 2009

El Servicio debe analizar en relación a lo ocurrido durante la revisión y mejoramiento del Proceso de Gestión de Riesgos y en base a la auditoría de aseguramiento realizado por el Auditor Interno del Servicio, si los roles definidos o reformulados durante el año 2008, responden en forma adecuada a los requerimientos del Proceso, examinando la necesidad de modificar roles, crear o eliminar instancias, mejorar la definición de responsabilidades, entre otros elementos.

Establecer un diccionario de riesgos: A nivel teórico y práctico se considera la necesidad de formular un diccionario de riesgos para la entidad. En este caso, como se trata de una entidad global (Sector Gubernamental), el diccionario de riesgos fue confeccionado por el Consejo de Auditoría Interna durante el año 2007 y remitido a todos los Servicios, para que lo utilicen.

Acciones año 2009

Durante el año 2009 y en general, siempre que sea necesario, el Servicio puede incorporar conceptos complementarios propios, a fin de hacer más completo el diccionario de riesgos.

1.2.- Contexto de gestión de riesgo

Para establecer el contexto de gestión debe establecerse y definirse el alcance de aplicación del análisis de riesgos.

A través de la documentación técnica del Consejo de Auditoría se ha definido que el Proceso de Gestión de Riesgos debe aplicarse a nivel de procesos, desagregados en subprocesos, etapas, actividades y riesgos específicos.

Dentro de la señalada desagregación en procesos, subprocesos y etapas, se agregan conceptos como la clasificación en procesos transversales en la Administración del Estado, la tipificación de riesgos y la ponderación porcentual de la importancia estratégica de los procesos y subprocesos

en la organización, que también deben ser incorporados dentro del contexto de la gestión de riesgos.

1.2.1.- Desagregación de procesos críticos y modelamiento de riesgos

Para levantar información de los procesos, la técnica a utilizar para documentar y estructurar el trabajo corresponde a la desagregación de la información en una matriz de riesgos. Esta técnica permite correlacionar la estructura desagregada de un proceso (proceso, subproceso y etapas) con los objetivos operativos, el nivel de riesgo, el nivel de eficiencia de los controles mitigantes y, finalmente, con el nivel de exposición al riesgo.

Esta técnica tiene las siguientes ventajas:

- Obliga a los funcionarios encargados a conocer e interactuar en forma integral con su organización.

- Permite construir la Matriz de Riesgos Estratégica de la organización y las matrices específicas para cada proceso relevante o materia específica que se requiera analizar.

- Se genera una sólida base para aplicar el Proceso de Gestión de Riesgos.

- Una vez identificados los procesos que desarrolla el Servicio se debe realizar la desagregación de procesos y el modelamiento de los riesgos y los controles.

Los procesos deben ser desagregados en todos los subprocesos que los componen, y éstos a su vez deben ser desagregados en todas las etapas que componen cada subproceso. Una guía básica para levantar procesos y los elementos que deben considerarse, se contiene en el anexo Nº 4 de este documento.

Desagregados los procesos, es necesario identificar los objetivos operativos de cada subproceso o etapa que los componen, (identificar cuál es la finalidad específica que se persigue en la generación de un producto o servicio), basándose para ello en las declaraciones formales del Servicio, en el análisis documental y en las entrevistas con los encargados de los procesos.

Identificados los objetivos operativos de la etapa o subproceso, deben identificarse los riesgos operativos que pueden afectarlos, entendiendo como tales, aquellas situaciones cuya ocurrencia u omisión pudieran afectar total o parcialmente el logro de los objetivos operativos.

Identificados los riesgos, debe calificarse su fuente y tipología de acuerdo a lo señalado al punto 1.2.4 de este documento.

Una vez identificados la fuente y tipología de los riesgos operativos, debe calificarse su severidad en términos de probabilidad e impacto, utilizando al efecto la metodología entregada por el Consejo de Auditoría u otra propia del Servicio previamente validada por ese organismo. (Tablas para valuación en el anexo Nº 5)

El próximo paso consiste en el reconocimiento y levantamiento de los controles que tiene el Servicio y que se orientan a mitigar los riesgos operativos identificados. En este punto, debe hacerse un análisis de los controles relevando sólo aquellos claves, cuyo objetivo es la mitigación

de los riesgos. Deben clasificarse y calificarse los controles, de acuerdo a su nivel de cumplimiento con las normas de control interno y según su oportunidad, periodicidad y automatización, utilizando para ello la metodología del Consejo de Auditoría u otra propia del Servicio, validada previamente por este Consejo. (Tablas para valuación se presentan en el anexo Nº 5)

Debe calcularse el nivel de exposición al riesgo, por riesgo, por etapa, por subproceso y finalmente por proceso. (Tablas para valuación se presentan en el anexo Nº 5)

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

- Desagregación de los procesos de la institución.
- Identificación de subprocesos en esos procesos.
- Identificación de etapas en cada subproceso.
- Identificación de los objetivos operativos por etapa o subproceso.
- Identificación de todos los riesgos operativos relevantes.
- Identificación de la fuente del riesgo y su tipología.
- Valor y clasificación de la severidad de los riesgos operativos.
- Identificación, valor y clasificación de la efectividad de los controles asociados al riesgo operativo.
- Valor de la exposición al riesgo individual, por etapa, subproceso y proceso crítico.

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

Acciones año 2009

Para el desarrollo del Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 – Nº 3, el Servicio debe revisar nuevamente la desagregación de procesos, subprocesos y etapas, así como los objetivos, riesgos y controles, determinando si esta desagregación y la identificación de riesgos y controles es adecuada y corresponde a la realidad del Servicio. Para esta revisión deberá considerar los resultados de la auditoría de aseguramiento y de las demás auditorías realizadas durante el año 2008, de acuerdo a la retroalimentación del Proceso de Gestión de Riesgos que a través de éstas se haya realizado.

1.2.2.- Procesos Transversales en la Administración del Estado

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

En el año 2008, los Servicios identificaron y revisaron la identificación de los procesos que desarrollan de acuerdo a las denominaciones propias de cada entidad, y la clasificación de esos

procesos en categorías mayores de procesos transversales en la Administración del Estado. (Megaprocesos)

Acciones año 2009

Para el desarrollo de este Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 – Nº 3, los Servicios, deberán seguir revisando la clasificación de sus procesos en procesos transversales. Estas categorías estaban establecidas en el Documento Técnico Nº 38/2008, sin embargo producto de las necesidades de los Servicios, se definieron algunos procesos transversales nuevos (destacados en el listado).

Los procesos transversales vigentes para el año 2009, se señalan en el siguiente cuadro Nº 2.

Cuadro Nº 2: Clasificación y descripción de Procesos Transversales en la Administración del Estado

Procesos Transversales en la Administración del Estado	Descripción
Procesos de negocio	
Subsidios a privados de fomento	Se entienden aquellos cuyo objetivo es la promover, mediante incentivos económicos, que los particulares realicen por sí mismos actividades productivas.
Subsidios a privados social	Se entienden como tales los procesos cuyo objetivo es la promoción de ciertos objetivos sociales como la integración, etc.
Subsidios a privados asistencial:	Consisten en procesos cuya finalidad es entregar ayuda de subsistencia a particulares.
Transferencias a / de otras entidades públicas	Son procesos en que, por ley o convenios, se entregan o reciben recursos de otro organismo del Estado.
Servicios de atención al ciudadano – contraprestación	Procesos que se orienten a servir a todos los ciudadanos a través de la entrega de atención, servicios o productos.
Servicios de atención social/ previsional /salud	Procesos que se orienten a prestar una atención de salud, previsional o social a personas que tengan ciertas calidades (Ej.: pensionados públicos, ancianos, personas de las fuerzas armadas, etc.)
Créditos - recuperación prestamos	Se refiere a procesos de entrega de préstamos, incluyéndose los procesos de planificación, ejecución y cobranzas.
Almacenamiento y distribución	Procesos que consistan en bodegaje, mantenimiento de stock y distribución de materiales o bienes.
Infraestructura	Procesos que se refieran a los bienes muebles e inmuebles del servicio que se utilizan para cumplimiento del rol del Servicio.
Asesoría a infraestructura	Procesos que impliquen estudios y acciones que apoyen decisiones sobre la infraestructura.
Estudios para marco cultural	Procesos de estudios culturales que releven las artes, literatura, pintura y todo lo relacionado a temas culturales.
Estudios para regulaciones, normativa y fijación tarifaria	Procesos de estudios que sirvan o puedan servir de base para la emisión de normativa, regulaciones, tarifas, etc.
Administración de bienes estratégicos	Proceso a través del cual el servicio gestiona aquellos bienes que son indispensables para el cumplimiento de su función; que son de la esencia de su "negocio".
Otorgamiento y/o reconocimiento de derechos	En el caso de aquellos servicios que entregan derechos o beneficios a personas naturales como ser parte de un registro, derechos de aguas, etc.
Mejoramiento de la gestión	Entendiendo todos aquellos proceso relacionados al PMG, convenios de desempeño y otros estímulos por metas.
Estudios e investigaciones	Aquellos estudios cuyo sentido es investigar un tema económico, financiero, de mercado u otra situación determinada importante para el Servicio.

Legal estratégico	Desarrollo de acciones legales y/o judiciales como negocio del Servicio.
Control de outsourcing	Equivalen a la gestión y monitoreo de los contratos que externalizan funciones propias del Servicio.
Seguridad y Control de Personas y/o Recintos	Proceso relacionado con seguridad que realizan determinados entes del estado en relación a las personas en distintas calidades: victimas, imputados, reos, reclutas y la ciudadanía en general. Esto podría incluir operaciones de distinta naturaleza como vigilancia, traslados, control u otros de índole distinta, relacionados con la seguridad.
Seguridad del transporte	Procesos relacionados con seguridad operacional y respuestas ante situaciones de emergencias de los servicios de transporte terrestre, marítimo y aéreo, así como de las instalaciones portuarias y aeroportuarias o de cualquier otra índole, en donde exista tráfico de pasajeros o carga.
Calificación ambiental	Procesos relacionados a análisis, autorizaciones y permisos medio ambientales.
Producción de bienes materiales	Corresponde a aquellos procesos productivos que generan bienes materiales como resultado
Comercialización	Procesos que desarrollan aquellos Servicios que venden productos y/o servicios a terceros.
Coordinación de Acciones de Emergencia (nuevo para el 2009)	Procesos asociados a la ejecución y coordinación de operaciones de emergencia, gestión de recursos para emergencias, monitoreo y análisis de los diversos factores y elementos relacionados con situaciones de emergencia o catástrofes.
Procesos gerenciales	
Planificación presupuestaria	Proceso anual que se realiza en el Servicio para programar la presupuestación de las diversas acciones que ejecuta.
Planificación estratégica	Proceso que realiza el servicio en el que fija sus objetivos, sus metas y la forma como las cumplirá.
Coordinación entre instancias	Procesos que implican relaciones entre diversos niveles, personas o entidades cuya organización y canalización son de responsabilidad del servicio.
Gobierno Electrónico	Procesos integrales para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar eficiencia y eficacia de la gestión pública e incrementar la transparencia del sector público y la participación de los ciudadanos a través del uso de las tecnologías de información y comunicaciones (TIC)
Inversión	
Iniciativas de inversión	Todos los procesos de inversión considerados en el subtítulo 31, desde los estudios a la ejecución.
Mercado financiero	Inversión en instrumentos financieros y de mercado accionario que realizan algunos Servicios autorizados.
Información	
Sistemas de información administrativos	Aquellos sistemas de información que entregan reportes y datos a los que puedan tener acceso terceros
Sistemas informáticos	Soporte informático interno del servicio, que comprende sistemas de información contable, financieros y operativos que contienen datos internos del Servicio.
Control operativo de los recursos públicos	
Fiscalización	Procesos a través de los cuales los Servicios controlan a entes externos en el cumplimiento de normas y estándares.
Evaluación y control de substancias	Proceso de control de substancias peligrosas.
Control de gestión	Proceso a través del cual el servicio controla el cumplimiento de las metas, logros e indicadores que se ha definido en su planificación.
Soporte	
Financiero	Procesos contables, de tesorería, registro presupuestario, etc.
Legal	Asesoría y apoyo jurídico dirigido al quehacer interno del Servicio.
Comunicaciones	Acciones de difusión y publicidad de los programas y acciones desarrolladas por el Servicio.

Adquisiciones y abastecimiento	Incluye la programación de compra, licitación, compra, recepción y distribución de los bienes y servicios adquiridos.
Recursos humanos	Incluye todos los procesos relacionados al personal, su capacitación, remuneraciones, feriados y bienestar.
Administración/mantenimiento recursos	Procesos de gestión de los recursos materiales del servicio, inventario, baja y traslado.
Gestión documental	Procesos de administración, dirección, manejo, registro, archivo y almacenamiento de documentación del Servicio, con o sin apoyo de sistemas informáticos, referido tanto a documentación interna como externa del Servicio.
Auditoría Interna	Proceso independiente y objetivo de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Se orienta a la prevención y contempla actividades de planificación, programación, ejecución, informe y seguimiento.

Es necesario relevar que los Servicios deben clasificar sus procesos sólo en una de las categorías antes definidas, basados en las características organizacionales y en los objetivos de éstos. Cuando existan dudas o diferencias respecto de la clasificación de uno o más procesos dentro de la categoría de procesos transversales, deberá consultarse y discutirse con el respectivo asesor de riesgos del Consejo de Auditoría.

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

Cuadro Nº 3: Ejemplo de clasificación de procesos

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

1.2.3.- Ponderación estratégica por proceso y subproceso

Debido a que el levantamiento a nivel de procesos corresponde al 100% de los que desarrolla el Servicio (negocio, estratégicos y soporte) y considerando que no todos los procesos tienen la misma importancia estratégica dentro de una Institución, debe realizarse una ponderación porcentual de cada proceso, que permita determinar el peso relativo que tiene cada uno en el logro de los objetivos estratégicos y la misión del Servicio. Esta ponderación por procesos, debe realizarse por la dirección del Servicio, en forma justificada, tomando en consideración variables como las siguientes:

- Nivel de contribución del proceso a la misión y objetivos estratégicos del Servicio.
- Impacto del proceso en la imagen del Servicio.
- Nivel de recursos que involucra cada proceso.
- Cobertura del proceso.

- Características de los usuarios, clientes y proveedores.
- Eficiencia de los sistemas de información del proceso.
- Complejidad y volatilidad de las actividades desarrolladas en el proceso.
- Dispersión geográfica de las operaciones desarrolladas en el proceso.
- Cambios organizacionales, operacionales, tecnológicos y económicos producidos en el proceso.

De la misma manera, ponderados estratégicamente los procesos, debe definirse por la dirección el peso relativo que cada subproceso tiene dentro de un proceso, esto, atendiendo a la relevancia o importancia estratégica que tiene cada subproceso en la consecución exitosa de los objetivos de cada proceso. Esta ponderación de los subprocesos al igual que la de los procesos debe ser justificada adecuadamente, considerándose para esta labor algunas variables como las siguientes:

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

La ponderación porcentual distribuida en todos los procesos en la institución debe sumar 100%, asimismo, la ponderación porcentual distribuidas en todos los subprocesos dentro de un proceso, debe sumar 100%.

Cuando existan dudas o diferencias que surjan respecto de la ponderación estratégica de los procesos o subprocesos, deberá consultarse y discutirse con el respectivo asesor de riesgos del Consejo de Auditoría.

Acciones año 2009

Para el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, y en general en forma periódica, los Servicios deben revisar y mejorar la forma cómo se ponderaron los procesos y subprocesos. El mejoramiento debe tener en consideración los siguientes puntos:

- Todos los procesos deben ponderarse.
- La ponderación de todos los procesos debe sumar cien por ciento (100%).
- La ponderación es reflejo de la importancia del proceso en el quehacer del Servicio, de ello que los procesos que generan productos estratégicos del Servicio, deberían tener mayor ponderación.
- La justificación debe fundamentarse en algún criterio de los antes mencionados, o bien en alguna variable objetiva definida por el Servicio: No basta señalar en qué consiste el proceso o subproceso, ni tampoco es suficiente indicar que se trata de un proceso clave al interior del Servicio, si no que es necesario señalar el por qué de su relevancia.

- Las ponderaciones de los subprocesos dentro de un proceso, deben sumar cien por ciento (100%).
- La ponderación de los procesos de negocios del Servicio debe ser mayor a la ponderación de los procesos de soporte.

A continuación en el cuadro Nº 4 se entrega a modo de ejemplo la ponderación de los procesos y subprocesos de una organización ficticia, con la justificación correspondiente:

Cuadro Nº 4: Ejemplo de justificación de la ponderación estratégica de procesos y subprocesos

Proceso	Pond.[2]	Justificación de la ponderación	Subprocesos	Pond.[3]	Justificación de la ponderación
Crédito de fomento para mujeres microempresarias	35%	Se trata del proceso principal del Servicio, que cumple el objetivo estratégico de entregar apoyo a las iniciativas de la mujer microempresaria, involucra sobre M$ 20.000, y se orienta a usuarias en situación vulnerable, con ingresos anuales inferiores a las 200 UF	Postulación crédito	10%	La ponderación baja considera que la postulación es un acción externa, propia de las usuarias
			Evaluación crédito	35%	Este subproceso es importante para el éxito del proceso por cuanto las deficiencias en la evaluación del crédito afectan la recuperación del mismo y la imagen del Servicio, por otra parte se trata de una labor altamente especializada, para la cual no siempre se cuenta con personal idóneo.
			Entrega crédito	20%	Su nivel de complejidad es medio, pero se le pondera con este porcentaje puesto que afecta la organización interna del Servicio pero su efecto no es directo en las usuarias o en la imagen
			Recuperación crédito	35%	La baja recuperación repercute en el presupuesto del Servicio, afectando directamente a las otras usuarias y la imagen del Servicio, además en la actualidad se hace manualmente y los errores en su registro son frecuentes
Capacitación para los negocios	25%	Proceso importante, ya que colabora al cumplimiento del el objetivo estratégico de entregar apoyo a las iniciativas de la mujer microempresaria, involucra un presupuesto superior a M$ 3.000 y se dirige a mujeres en situación vulnerable con baja escolaridad	Postulación	20%	Se trata de un beneficio conocido por la población objetivo, del cual se realiza difusión desde hace seis años con buena respuesta de las usuarias. El personal tiene experiencia y se cuenta con un sistema de información para el ingreso y validación de datos de los postulantes
			Capacitación	50%	Se trata de cursos contratados en el mercado, entregados por personal externo al Servicio, que debe ser monitoreado a fin que entregue materias requeridas por las usuarias, con un nivel comprensible para el público objetivo, con la flexibilidad necesaria para mujeres y no siempre se cuenta con personal adecuado y recursos para la supervisión

[2] Porcentaje de Ponderación Estratégica de los procesos en relación con los objetivos estratégicos y la misión de la institución.
[3] Porcentaje de Ponderación Estratégica de los subprocesos en relación con los objetivos del proceso.

			Evaluación	30%	Es importante ya que es la forma de medir como se ha recibido por las usuarias los contenidos de los cursos y evaluar los resultados de los cursos. No se cuenta con personal idóneo en todas las materias para hacer la evaluación del curso y una mala capacitación afecta la imagen del Servicio
Presupuesto y Contabilidad	10%	…….	…….	…….	……..

1.2.4.- Tipología de riesgos

En el marco del levantamiento de procesos, debe utilizarse una tipología o categorización de riesgos. En estas categorías deben clasificarse los riesgos específicos que se identifiquen en la próxima fase. La tipología de riesgos, sirve para agrupar aquellos riesgos que tienen características y elementos comunes.

En relación a la fuente u origen de los riesgos, se pueden señalar que existen riesgos de fuente externa y riesgos de fuente interna[4]. Los riesgos de fuente externa, son aquellos que tienen su origen en situaciones que están fuera de la administración y control del Servicio, como los cambios políticos y sociales. Al contrario, son de fuente interna, los que se originan al interior del Servicio, como los relacionados a las capacidades del personal y a la efectividad de los sistemas de información.

En el cuadro Nº 5, se señalan ejemplos de los tipos de riesgos, considerando los elementos que caracterizan a cada uno. Es necesario señalar, que la clasificación propuesta, es una adaptación de la establecida en el Modelo COSO II, que se ha modificado para ser aplicada en el Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 – Nº 3.

Cuadro Nº 5: Ejemplos de tipificación de riesgos

Tipos de Riesgos	Elementos que los caracteriza	Ejemplos de riesgos específicos
Económicos	Se relacionan con elementos financieros, comerciales y presupuestarios	- Falta de disponibilidad presupuestaria - Modificaciones presupuestarias por deficiente ejecución - Errores en el servicio de la deuda - Servicio de la deuda muy alto - Exceso de compromisos del Servicio que afecten su presupuesto - Malas inversiones en mercado de capitales - Deficiencias en la ejecución presupuestaria del Servicio - Falta de Suplementos del Ministerio de Hacienda o falta de oportunidad en los mismos.
Sociales	Se relacionan con elementos de comunidad social, cultural, demográfica, comportamientos sociales.	- Deficiente comportamiento de usuarios (bajo compromiso, bajo cumplimiento, etc.) - Problemas con los datos personales y privados de los clientes o proveedores - Falta de responsabilidad social del Servicio o

[4] Cfr. COSO II

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

Sistemas	Relacionado con los sistemas de información del Servicio, las tecnologías que posee y los datos que maneja.	- Falta de integridad y confiabilidad de datos - Falta de disponibilidad de datos y sistemas - Deficiencias en la selección de sistemas - Deficiencias en el desarrollo y despliegue de los sistemas - Deficiencias en el mantenimiento - Falta de interoperabilidad de los sistemas

Acciones año 2009

Para el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, y en general en forma periódica, el Servicio debe revisar y mejorar la forma cómo calificó los procesos de acuerdo a su origen y tipología. El mejoramiento debe tener en consideración los siguientes puntos:

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

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

2.- FASE IDENTIFICACIÓN DE RIESGOS Y OPORTUNIDADES

La metodología del Consejo de Auditoría, considera la identificación de riesgos y oportunidades que pueden afectar la consecución de los objetivos estratégicos del Servicio. 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.

Los eventos pueden generar impactos positivos o negativos, o ambos. Los impactos positivos, se denominan oportunidades, y los negativos son conocidos como riesgos.[5]

Como puede apreciarse, la identificación de eventos consta de dos aspectos. Por una parte, la identificación de oportunidades y por otra la identificación de riesgos.

2.1.- Identificación de oportunidades

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

[5] De acuerdo a COSO II, los eventos son todas aquellas circunstancias que pueden afectar la consecución de los objetivos estratégicos de una organización. Las que lo afectan en forma positiva se denominan oportunidades y las que afectan en forma negativa, se denominan riesgos.

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

A continuación, en el cuadro Nº 6 se entrega un ejemplo de identificación de oportunidades a través de eventos.

Cuadro Nº 6: Ejemplo de identificación de oportunidades por proceso

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

Acciones año 2009

Para el cumplimiento del Objetivo Gubernamental Nº 3 del año 2009 / Primer Trimestre año 2010 será necesario identificar oportunidades a nivel global de procesos. Es importante que se realice esta actividad, puesto que las oportunidades sirven a la institución para retroalimentar las estrategias. El formato en el que deben reportarse más adelante**,** al punto IX, resumen de requerimientos específicos para el Objetivo Gubernamental de Auditoría 2009/Primer Trimestre año 2010 – Nº 3.

2.2.- Identificación de riesgos

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

Acciones año 2009

Para cumplir el Objetivo Gubernamental 2009/Primer Trimestre año 2010 – Nº 3, el Servicio debe revisar y mejorar su identificación de riesgos y oportunidades, poniendo especial énfasis en los siguientes puntos:

- Actualizar los riesgos, considerando los cambios normativos, presupuestarios o de los lineamientos del Gobierno o dirección.
- Identificar en la forma más completa y desagregada posible los riesgos que se relacionan a una etapa dentro de un proceso. Para ello se sugiere examinar las actividades al interior de las etapas, identificando los riesgos que se asocian a dichas actividades.
- Considerar que una etapa puede tener, y en general es así, más de un riesgo.
- Considerar que una buena y completa descripción del objetivo operativo de la etapa facilita la identificación de riesgos.
- Mejorar en forma especial respecto de los controles:

    - Identificar controles claves (Ver definición en el Anexo Nº 9)
    - Mejorar la descripción de los controles, señalando la norma o guía que lo instruye, quién lo realiza, qué actividades desarrolla, cómo las ejecuta y cuándo y cómo se evidencia su cumplimiento (registros documentales o registros electrónicos en el sistema).
    - Considerar que los controles que se identifican deben estar directamente relacionados con el riesgo que supuestamente mitiga.

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

Acciones año 2009

Para el cumplimiento del Objetivo Gubernamental de Auditoría se debe señalar, de acuerdo a la tipología entregada, a qué tipo genérico de riesgo corresponde el riesgo específico determinado y cuál es su fuente (externa o interna), como se señala a continuación en el ejemplo del cuadro Nº 7.

Cuadro Nº 7: Ejemplo de clasificación de riesgos de acuerdo a su tipología

Proceso Transversal	Proceso	Pond.	Subproceso	Pond.	Etapas	Objetivos	Riesgos específicos	Fuente de Riesgos	Tipo de riesgo	Prob.	Cons.	.....
Créditos – Recuperación de préstamos	Créditos de fomento a mujeres microempresarias	30%	Recuperación del crédito	25%	Cobranza	Recuperar oportunamente los créditos	Falta de acciones oportunas de cobranza	Interna	Procesos	3	3	…
							Insolvencia de los deudores	Externa	Económico	2	4	…
						Contar con garantías de los créditos	Falta de garantías	Interna	Procesos	1	4	…
					Ingreso fondos recuperados	Ingresar los fondos recuperados en forma oportuna y completa	Ingreso inoportuno o incompleto de pagos	Interna	Personas	4	3	…
							Errores en la digitación de los montos	Interna	Personas	3	4	…
							Problemas en la transformación de la información del sistema del Servicio al SIGFE	Interna	Tecnológico	2	4	…
---	…	…	…	…	…	…	…	…	…	…	…	…
---	…	…	…	…	…	…	…	…	…	…	…	…

Para el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 - Nº 3, deberá revisarse la clasificación de los riesgos realizada de acuerdo a la tipología desplegada en el cuadro Nº 5 anterior, prestando especial atención a dos puntos específicos:

a) Los riesgos deben ser clasificados según su fuente como externos o internos. Para ello debe estarse principalmente al origen del riesgo, esto es a su causa. Por ejemplo: si existe un riesgo relacionado con la mala calidad de los datos e información del Servicio, nos encontramos con un riesgo de origen interno, independientemente que la administración del sistema de información se haya externalizado, ya que el riesgo parte de una debilidad interna. En cualquier caso, debe clasificarse sólo en una fuente, no siendo válido un riesgo interno /externo, debiendo optarse por aquella fuente que tenga mayor importancia en el origen del riesgo.

b) Los riesgos deben ser clasificados sólo en una de las tipologías definidas en este documento técnico. Para ello, debe considerase principalmente la causa del mismo. Por ejemplo, si se identifica un riesgo de corrupción o de falta de probidad en el personal, nos encontramos con un riesgo que se clasifica en la tipología "personas" aún cuando sus consecuencias afectan también a la imagen del Servicio.

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

2.3.- Identificación de riesgos relacionados con el Gobierno Electrónico: En la actualidad el Gobierno Electrónico constituye una gran herramienta para la modernización del Estado, las tecnologías de la información son el instrumento adecuado para proveer la participación del ciudadano en las instancias de Gobierno y la transparencia en el quehacer del Estado. En este panorama, Chile no se ha quedado atrás y desde el año 2004 viene fortaleciendo y promocionando el uso de tecnología para hacer un Gobierno más eficiente, transparente y participativo.

De acuerdo a lo señalado en el párrafo anterior, los Servicios deben, para actualizar su gestión, incorporar aquellos procesos y riesgos relacionados con el Sistema de Gobierno Electrónico.

Para identificar los procesos relacionados con el Gobierno Electrónico y realizar el análisis de los riesgos que los pueden afectar, es necesario considerar que éste consiste en el uso de las tecnologías de información y comunicaciones (TIC) que realizan los órganos de la administración para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y la eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público, así como la participación de los ciudadanos[6].

Dentro del Programa de Mejoramiento de la Gestión, existe el Sistema de Gobierno Electrónico. Este sistema, consta de cuatro etapas, que consideran, diagnostico, planificación implementación y evaluación, respectivamente.

Para el levantamiento de procesos críticos de Gobierno Electrónico del Servicio, se sugiere:

- En base a lo implementado en el marco del PMG de Gobierno Electrónico del Servicio, revisar, conocer y analizar, cuáles procesos, de provisión y de soporte, fueron seleccionados como elegibles para desarrollar proyectos que mejoren dichos procesos a través de la incorporación de TIC, con el objeto de favorecer mejoras en la gestión, entregar

[6] Fuente: Instructivo Presidencial Gobierno Electrónico, Mayo 2001.

una mejor atención ciudadana y/o un fortalecimiento de la democracia. (Etapa I, Diagnóstico y Etapa II Planificación, Sistema de Gobierno Electrónico).

- De esos procesos seleccionados, analizar cuáles fueron implementados o serán implementados, de acuerdo a los proyectos planificados, distinguiendo procesos de negocio (provisión) y de soporte. (Etapa III Implementación y Etapa IV Evaluación, Sistema de Gobierno Electrónico).

- Una vez determinados cuáles fueron los procesos que se implementaron, debe verificarse el levantamiento de los mismos.

- El Servicio, dentro del marco PMG Gobierno Electrónico, tuvo que realizar un levantamiento de los procesos, estableciendo diagramas, y descripción de las actividades, análisis de los problemas u oportunidades, las propuestas de modificaciones con la conceptualización de la solución, la presentación de herramientas tecnológica y la determinación de viabilidad del proyecto.

- En base a lo anterior, se debe analizar la documentación de ese levantamiento y, en conjunto con los encargados o dueños de proceso, desagregar los procesos, identificando a través del diagrama y otra documentación, los subprocesos, etapas y actividades de cada proceso de acuerdo con la metodología dispuesta por el Consejo de Auditoría.

- Una vez realizada la desagregación de los procesos de Gobierno Electrónico, es necesario que en conjunto con los encargados o dueños de procesos, se identifiquen los objetivos operativos de las etapas desagregadas.

- Identificados los objetivos operativos, deben identificarse los riesgos asociados a las actividades de cada etapa. Hay que relevar que, una parte de esta labor, fue realizada por los encargados de los procesos, en el marco del PMG de Gobierno Electrónico al definir los problemas dentro del levantamiento. Sin perjuicio de lo anterior, este análisis debe enriquecerse, en base a la desagregación realizada y en relación a los nuevos riesgos que el mejoramiento tecnológico le impone a este proceso.

En el anexo Nº 8, a modo ilustrativo, se presentan algunos ejemplos de riesgos genéricos que pueden afectar los procesos que incorporan Tecnología de la Información.

Acciones año 2009

Para el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, el Servicio debe volver a revisar y actualizar la identificación de riesgos relacionados con el Gobierno Electrónico. Para ello se sugiere analizar y actualizar cuáles procesos dentro del Servicio, han sido mejorados con TIC[7] y dentro de éstos examinar cuáles son los riesgos nuevos que surgen producto de este mejoramiento. Otra posibilidad es analizar Gobierno Electrónico como un proceso separado en forma integral.

Es necesario relevar que Gobierno Electrónico no es sinónimo de sistema de información, sino que se refiere al uso de tecnologías de información por parte del Estado para mejorar la calidad y

[7] TIC= Tecnologías de Información.

oportunidad de la información que se le entrega al ciudadano, su participación y la transparencia en el quehacer.

3.- FASE ANÁLISIS DE RIESGOS

3.1.- Análisis general de riesgos

Los Servicios han desarrollado la identificación de riesgos específicos y su análisis en los últimos años, en el marco de la confección de la Matriz de Riesgos Estratégica, examinando los riesgos en relación a su probabilidad y consecuencias y los controles en términos de efectividad, para finalmente identificar el nivel de exposición al riesgo por proceso, subproceso, etapa y riesgo específico. Sin embargo lo anterior, en esta fase, existen dos elementos que deben considerarse para complementarla.

3.1.1.- Actualización de la identificación de los riesgos: Los Servicios deberán poner al día su análisis de riesgos, actualizando la Matriz de Riesgos Estratégica e incorporando los procesos relacionados con el Gobierno Electrónico y todos aquellos procesos nuevos que desarrolle el Servicio, con sus respectivos riesgos y controles.

Acciones año 2009

Para cumplir el Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, y en general para un buen desempeño del Proceso de Gestión de Riesgos, el Servicio debe revisar y mejorar su análisis de riesgos y oportunidades, poniendo especial énfasis en los siguientes puntos:

- Actualizar los riesgos y su calificación de probabilidad e impacto, de acuerdo a las últimas auditorías, los antecedentes históricos que se tengan y a los cambios que hayan afectado a la institución (modificaciones presupuestarias, nuevos objetivos, eliminación de programas, cambios en las políticas gubernamentales, modificaciones en la orientación y lineamientos de la dirección, entre otras situaciones).
- Considerar la retroalimentación de la auditoría interna, ya sea a través de las auditorias de aseguramiento y seguimiento del Proceso de Gestión de Riesgos, así como las auditorías a los diversos procesos del Servicio.
- Actualizar los riesgos de Gobierno Electrónico, analizando qué procesos han sido mejorados con TIC y cómo ello influye en su desarrollo, teniendo en consideración que muchas veces el mejoramiento de las TIC se realiza en etapas o actividades del proceso, pero su influencia e impacto irradia la totalidad del mismo.
- Relacionar adecuadamente los riesgos con el objetivo de la etapa. Esto implica que la concreción de un riesgo debe afectar el cumplimiento o logro de la etapa en forma directa, de tal manera que los riesgos identificados impidan o dificulten el resultado esperado por el Servicio al desarrollar esa etapa.
- Actualizar la descripción de los controles de acuerdo a los resultados de las auditorías realizadas, los antecedentes históricos que se tengan y a los cambios que hayan afectado a la institución (modificaciones presupuestarias, nuevos objetivos, eliminación de programas, entre otras situaciones). Ver anexo Nº 9.
- Ajustar las exposiciones al riesgo de acuerdo a las actualizaciones realizadas a los riesgos y controles.

3.1.2.- Incorporación del concepto de ponderación estratégica: Como ya se señaló en el punto Nº 1 de este documento, Fase de Establecimiento del Contexto; debe aplicarse el concepto de ponderación estratégica a nivel de proceso y subproceso. En efecto, para determinar el nivel de exposición al riesgo de los subprocesos y procesos, deberá multiplicarse el nivel de exposición final por proceso y subproceso[8] por el porcentaje de ponderación estratégica que a cada uno de ellos les fue asignado, de la forma que se explica en el cuadro a continuación:

Cuadro Nº 8: Ejemplo de ponderación estratégica por proceso y subprocesos

Proceso Transversal	Proceso	Pond[9]	Subproceso	Pond. 10	Etapas	...	Nivel de Exposición al Riesgo				Nivel de Exposición al Riesgo Ponderada	
							Riesgo Específico	Etapa	Subproceso	Proceso	Subproceso	Proceso
Proceso Transversal 1	Proceso 1	**50%**	Subproceso 1	70%	Etapa 1		3	3	3	2,8	3 x 70% = **2,1**	2,8 x 50% = **1,4**
					Etapa 2		3	3				
			Subproceso 2	30%	Etapa 3		3	3	2,5		2,5 x 30% = **0,75**	
					Etapa 4		2	2				
Proceso Transversal 2	Proceso 2	**20%**	Subproceso 3	60%	Etapa 5		5	5	3,5	3,8	3,5 x 60% = **2,1**	3,7 x 20% = **0,74**
					Etapa 6		2	2				
			Subproceso 4	40%	Etapa 7		2	2	4		4 x 40% = **1,6**	
					Etapa 8		6	6				
Proceso Transversal 3	Proceso 3	**30%**	Subproceso 5	50%	Etapa 9		2	2	2	2,7	2 x 50% = **1**	2,7 x 30% = **0,81**
					Etapa 10		2	2				
			Subproceso 6	50%	Etapa 11		2	2	3,3		3,3 x 50% = **1,65**	
					Etapa 12		4	4				
					Etapa 13		4	4				

Del cuadro Nº 8, es posible apreciar que la ponderación estratégica releva la importancia del proceso en el contexto de la Institución y del subproceso en el contexto del proceso, acercando el resultado a la posición y relevancia de éstos. En efecto, en el ejemplo se observa que sin aplicar el porcentaje de ponderación estratégica, aparece como de mayor nivel de exposición al riesgo (y por tanto, aparentemente como más prioritario para actuar sobre él) el proceso 2, sin embargo, aplicando la ponderación estratégica definida por la dirección aparece como de mayor prioridad el proceso 1, el cual, de acuerdo a la determinación realizada por la dirección es el más importante al interior del Servicio.

Acciones año 2009

Para el Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, el Servicio debe nuevamente revisar y mejorar las ponderaciones, de acuerdo a lo señalado en el punto 1.2.2 de este documento (Ponderación estratégica por proceso y subproceso), teniendo presente que los cambios de políticas de Gobierno, las modificaciones presupuestarias y la orientación en los lineamientos de la Dirección, las afectan directamente.

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

4- FASE EVALUACIÓN DE LOS RIESGOS

La Fase de Evaluación de los Riesgos en la metodología del Consejo de Auditoría Interna considera dos pasos. Primero la definición del criterio que se escogerá y segundo la confección de un ranking de riesgos en la organización.

4.1.- Definición de criterios

En este caso se utilizará el criterio asociado al nivel de exposición al riesgo, esto es el riesgo residual que subsiste después de aplicados todos los controles claves existentes. Para el desarrollo del Objetivo Gubernamental, el nivel de exposición al riesgo debe considerar la ponderación estratégica de procesos y subprocesos, de acuerdo a lo señalado en los párrafos anteriores. Esto implica que el criterio considerado para la evaluación del riesgo es el de exposición al riesgo ponderada. (Exposición al riesgo X ponderación estratégica)

En el cuadro Nº 9 se muestra la relación entre los distintos componentes del análisis de riesgos,

Cuadro Nº 9: Relación entre Severidad del Riesgo y Exposición al Riesgo

4.2.- Ranking de Riesgos

Ranking de Riesgos para priorización de estrategias

Basado en la información contenida en la Matriz de Riesgo Estratégica construida en las fases anteriores del proceso, se debe evaluar en cuáles ámbitos organizacionales se requiere actuar en forma prioritaria (procesos y subprocesos).

Para dar cumplimiento a esta tarea, la organización debe construir un Ranking de Riesgos en base al nivel de exposición al riesgo ponderada, con un alcance y criterios que se detallan en los puntos a y b siguientes:

a.- Ranking de procesos por nivel de exposición al riesgo ponderada

En el cuadro Nº 10 se presenta el esquema del análisis a realizar para un proceso desagregado hasta el nivel de riesgo específico.

Cuadro Nº 10: Ejemplo de Matriz de Riesgos por nivel de exposición al riesgo y nivel de exposición al riesgo ponderada (Sin perjuicio del formato electrónico en MS Excel que debe enviarse al Consejo de Auditoría en la fecha indicada)

Proceso Transversal	Proceso	Pond.[11]	Subproceso	Pond.[12]	Etapas	Objetivos	Riesgos	...	Severidad del Riesgo	Exposición al Riesgo por Sub proceso		Exposición al Riesgo por Proceso	
									E. R.	E.R. [13]	E.R. P[14]	E.R.	E.R.P
Créditos - recuperación préstamos	Entrega créditos	35%	Subproceso 1	60%	Etapa 1	...	...	...	3	3	1,8	2,8	0,98
					Etapa 2	...	...	...	3				
			Subproceso 2	40%	Etapa 3	...	...	...	3	2,5	1		
					Etapa 4	...	...	...	2				
Financiero	Contabilidad y presupuesto	10%	Subproceso 3	50%	Etapa 5	...	...	...	5	3,5	1,7	3,8	0,38
					Etapa 6	...	...	...	2				
			Subproceso 4	50%	Etapa 7	...	...	...	2	4,0	2		
					Etapa 8	...	...	...	6				
Subsidio a privados social	Capacitación	25%	Subproceso 5	50%	Etapa 9	...	...	...	2	2,0	1,0	2,7	0,67
					Etapa 10	...	...	...	2				
			Subproceso 6	50%	Etapa 11	...	...	...	2	3,5	1,7		
					Etapa 12	...	...	...	4				
					Etapa 13	...	...	...	4				
					Etapa 14	...	...	...	4				
Recursos Humanos	Recursos Humanos	10%	Subproceso 7	35%	...	...	...	...	...	...	...	...	...
			Subproceso 8	65%	...	...	...	...	...	...	...	...	...
.....	.....	20%	Subproceso 9	35%	...	...	...	...	...	...	...	...	...
			Subproceso 10	40%	...	...	...	...	...	...	...	...	...
			Subproceso 11	25%	...	...	...	...	...	...	...	...	...

Del ejemplo de matriz de riesgos expuesta (presentada en forma simplificada), emana el ranking que se presenta en el siguiente cuadro Nº 11, de acuerdo al nivel de exposición al riesgo ponderado.

[11] Ponderación estratégica del proceso, en relación a la misión y objetivos estratégicos del Servicio
[12] Ponderación estratégica del subproceso en relación a los objetivos del proceso.
[13] Exposición al Riesgo
[14] Exposición al Riesgo Ponderada

Cuadro Nº 11: Ejemplo de Ranking de procesos por nivel de exposición al riesgo ponderada

Procesos	Nivel de Exposición al Riesgo Ponderada	Ranking para priorizar estrategias de tratamiento de los riesgos en los Procesos
Entrega Créditos	0,98	**1º**
Capacitación	0,67	**2º**
Contabilidad y Presupuesto	0,38	**3º**
……		

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

b.- Ranking de subprocesos por nivel de exposición al riesgo ponderado

Una vez priorizados los procesos para los cuales se comenzarán a formular y aplicar las estrategias de tratamiento de riesgos, se debe priorizar por subprocesos que componen esos procesos, en base al nivel de exposición al riesgo ponderado, tal como se explicara anteriormente.

De esta manera, el ranking podría aparecer como sigue:

Cuadro Nº 12: Ejemplo de Ranking de Subprocesos por Nivel de Exposición al Riesgo Ponderado

Proceso	Subprocesos	Nivel de Exposición al Riesgo Ponderado por subproceso	Ranking para priorizar estrategias de tratamiento de los riesgos en los subprocesos
Entrega Créditos	Subproceso 1	1,8	**1°**
	Subproceso 2	1,0	**2°**
Capacitación	Subproceso 2	1,7	**1°**
	Subproceso 1	1,0	**2°**
…	…	…	…

Este ranking indica que se debe comenzar a tratar los riesgos asociados a los subprocesos 1 y 2 del proceso entrega de créditos y así sucesivamente con los demás.

Dentro de los subprocesos priorizados deben ser tratados los riesgos, correspondientes a las actividades que se desarrollan al interior de las etapas, así como los riesgos asociadas a las actividades de entrada y salida, priorizados de acuerdo al nivel de exposición al riesgo de cada etapa.

Acciones año 2009

Para el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, el Servicio debe revisar y mejorar su evaluación de riesgos, ajustando el ranking de procesos de acuerdo a la actualización realizada en la identificación y análisis de riesgos y controles. Por otra parte, también debe ajustar el ranking de subprocesos de acuerdo al cuadro Nº 12 anterior.

5.- FASE TRATAMIENTO DE LOS RIESGOS

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

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

5.1.- Formular estrategias para el tratamiento y monitoreo de los riesgos

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

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

5.2.- Estrategias genéricas para tratamiento de los riesgos

La teoría de Gestión de Riesgos señala que existen cuatro estrategias globales que permiten enfrentar la problemática de gestionar los riesgos, desde el punto de vista de su nivel de severidad (probabilidad y consecuencias) y del nivel de la exposición al riesgo (severidad – efectividad control), estas estrategias globales o genéricas son:

- **Evitar:** Salir de las actividades que generen los riesgos. Cuando esto sea realizable y no afecte los requerimientos legales o la eficiencia operacional. Esta estrategia en el sector público no es simple de aplicar, debido a que la mayoría de su quehacer se encuentra normado en sus leyes orgánicas u otros cuerpos legales

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

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

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

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

Cuadro Nº 13: Ejemplos de medidas para tratar el riesgo desde el punto de la severidad del riesgo y de la exposición al riesgo

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

5.3.- Evaluar y seleccionar las estrategias de tratamiento de los riesgos

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

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

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

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

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

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

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

En el cuadro Nº 14 se presenta una relación comparativa de la aplicación de las estrategias y su efecto potencial en la severidad del riesgo y en la efectividad del control.

Cuadro Nº 14: Relaciones generales entre las estrategias y su efecto en el riesgo y efectividad del control

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

5.4.- Preparar e implementar planes de tratamiento y monitoreo

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

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

Acciones año 2009

Para este año, el Servicio debe confeccionar un nuevo Plan de Tratamiento de Riesgos, considerando el ajuste del ranking y los nuevos resultados producto de la revisión del levantamiento de procesos, subprocesos y etapas y de la identificación de riesgos y controles. Este Plan de Tratamiento deberá realizarse teniendo en consideración los siguientes puntos:

- Los riesgos escogidos para el tratamiento deben ser adecuados para gestionar el riesgo del o los procesos priorizados.
- Las estrategias escogidas deben ser: reducir, aceptar, compartir o evitar, teniendo presente que las estrategias de aceptar o evitar, no tienen efecto sobre la severidad del riesgo o la efectividad del control.
- Las acciones definidas deben ser aptas para mitigar el riesgo al cual se asocian.
- Los indicadores deben ser de resultado y señalar explícitamente qué es lo que se quiere medir. Debe expresarse como una medida y establecer las variables y operaciones que se deben realizar para el cálculo del indicador.
- La meta debe ser el valor deseado del indicador que se espera alcanzar.
- El verificador debe ser apto para dar seguridad de que se alcanzó la meta.

Para mayor claridad de los puntos anteriores, ver un ejemplo en anexo Nº 10.

Con esta revisión y mejoramiento deberá emitirse un nuevo Plan de Tratamiento, que debe ir en el formato del cuadro Nº 15 siguiente y, que contendrá las medidas a adoptarse ante los riesgos no considerados en el Plan anterior o aquellos en que no se hayan concretado las acciones comprometidas.

Cuadro Nº 15: Formato para informar de los planes de tratamiento de los riesgos priorizados

Proceso transversal (1)	Proceso (2)	Ranking de procesos (3)	Subproceso (4)	Etapa (5)	Riesgo Específico (6)	Fuente del riesgo (7)	Tipo de riesgo (8)	Estrategia genérica (9)	Descripción de la estrategia a aplicar (10)	Efecto potencial en la severidad de riesgo y/o efectividad del control (11)	Responsable de la estrategia (12)	Plazo (13)	Indicador de logro (14)	Periodo Medición del Indicador (15)	Meta (16)	Evidencia que se observará (17)

Descripción de la información solicitada en el formato dispuesto en el cuadro Nº 15	
Número de descriptor	**Significado**
(1)	Proceso genérico, transversal o megaproceso al cual corresponde el proceso priorizado, de acuerdo a la clasificación del documento (Cuadro Nº 2).
(2)	Denominación específica que el proceso tiene en el Servicio.
(3)	Prioridad de tratamiento del proceso, de acuerdo a la ponderación que tienen el proceso en relación a la misión del Servicio.
(4)	Subprocesos que conforman el proceso priorizado.
(5)	Etapas que conforman cada uno de los subprocesos del proceso priorizado.
(6)	Riesgos que se identifican en la etapa, en relación a actividades que en dicha etapa se llevan a cabo.
(7)	Origen externo o interno de los riesgos, de acuerdo al control que tiene el Servicio de la fuente que los produce.
(8)	Clasificación del riesgo, de acuerdo a la tipología que entrega el documento en el cuadro Nº 5.
(9)	Tipo de estrategia que se adoptó para tratar ese riesgo de acuerdo al punto 5.2 (evitar, reducir, compartir, aceptar).

(10)	Detalle de la estrategia genérica que se va a utilizar. Pormenorizar las acciones y actividades que se desarrollarán para llevar a cabo la estrategia genérica.
(11)	Señalar si la estrategia apunta a disminuir la severidad del riesgo (probabilidad, impacto o ambos) y/o a potenciar el control y de qué manera.
(12)	Señalar quien es la persona o cargo responsable de la implementación de las acciones específicas de la estrategia.
(13)	Definir en qué plazo se debe implementar la estrategia.
(14)	Corresponde a la forma cuantitativa o cualitativa como se evalúa el nivel de cumplimiento de la estrategia definida. Debe tratarse de un indicador de resultado, que demuestre cómo la estrategia mitiga el riesgo al cual se asocia.
(15)	Señalar periodos en que se va a medir el indicador dependiendo de la naturaleza del mismo (mensual, trimestral, semestral, etc.)
(16)	Resultado tangible que se espera lograr con la implementación de la estrategia.
(17)	Documento o instrumento que se utilizará en la medición del indicador.

6.- FASE MONITOREO Y REVISIÓN

En esta fase es necesario nombrar responsables de monitorear la efectividad de todos los pasos del Proceso de Gestión de Riesgos, para asegurar que se está cumpliendo adecuadamente y que las circunstancias cambiantes no alteran las prioridades al afectar las ponderaciones estratégicas, las probabilidades o impactos de los riesgos, etc.

Para esta fase del Proceso de Gestión de Riesgos, el Servicio debe establecer formalmente responsables del monitoreo y formular estructuras de reportes útiles a la organización, que le permita a la dirección, obtener información relevante, en forma oportuna y periódica sobre el estado de los riesgos en cualquier etapa del proceso.

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

Actividades recomendadas para controlar los planes de tratamiento y monitoreo

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

Acciones año 2009

Para el año 2009, la institución deberá realizar el monitoreo en base al Plan de Tratamiento que definió y acompañó al Consejo de Auditoría al 30.10.08, para ello deberá utilizar el formato definido por el Formato Nº 16 de este Documento Técnico.

Cuadro Nº 16: Formato básico para informar del monitoreo de las estrategias de tratamiento de los riesgos

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

Descripción de la información solicitada en el formato dispuesto en el cuadro Nº 16 (sólo aquellos conceptos no explicados con ocasión del formato Nº 15)	
Número de descriptor	**Significado**
(a)	Señalar en qué fecha se evaluó la implementación de la estrategia
(b)	Señalar el resultado que se obtuvo de la medición de las metas. (cumplida, parcialmente cumplida, porcentaje de cumplimiento, etc.)
(c)	Expresar y detallar en que documentos o que información se utilizó para tener evidencia suficiente y adecuada del cumplimiento.
(d)	En caso de no haberse cumplido totalmente la meta, como se proyecta que será el cumplimiento. (en unidades de tiempo, o si no se podrá cumplir)
(e)	Sugerencias que realiza el responsable del monitoreo y revisión para que se obtenga el logro de la meta, o se mejore en términos de oportunidad y calidad.

7.- FASE COMUNICACIÓN Y CONSULTAS

Esta fase se desarrollará a través de comunicar, informar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos, interpretando al proceso como un todo. La información es identificada, capturada y comunicada de manera que todos puedan cumplir con sus responsabilidades.

La idea es que los interesados internos (el Servicio) y los externos que corresponda, estén informados de la marcha del Proceso de Gestión de Riesgos y de qué manera se van implementando las medidas para el tratamiento de riesgos. Para esto es importante que los informes y sistemas de información ofrezcan suficientes datos relevantes para posibilitar una comunicación y control eficaz. De tal manera, es conveniente contestar a las siguientes preguntas respecto de la información del Proceso de Gestión de Riesgos:

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

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

Es importante reiterar que el desarrollo de cada una de las fases del Proceso de Gestión de Riesgos es en primer lugar responsabilidad del Jefe Superior del organismo y luego también es

responsabilidad de todos los ejecutivos responsables de cada proceso y finalmente de todo el personal. La auditoría interna por su parte, debe apoyar a la referida autoridad a coordinar la implantación del proceso y a monitorear su adecuado avance en las diferentes fases, sin perjuicio de las actividades de aseguramiento contempladas en el Plan Anual aprobado por la dirección.

Acciones año 2009

Para cumplir el Objetivo Gubernamental 2009/Primer Trimestre 2010 – Nº 3, el Servicio deberá revisar la propuesta sobre información del Proceso de gestión de Riesgos que fue remitida al Consejo de Auditoría y mejorarla de forma que refleje un uso adecuado de la información que emana de dicho proceso.

Como sugerencia para mejorar la fase de comunicación y consulta, se recomienda a los Servicios, que no lo tengan, crear mecanismos para automatizar el análisis de la información del Proceso de Gestión de Riesgos, mediante el uso de la información derivada de la Matriz de Riesgos Estratégica y el establecimiento de relaciones e indicadores que permitan a través de consultas realizar análisis cuantitativos y cualitativos de la información, como por ejemplo a través de la importación de los datos a MS Excel o MS Access.

Algunos ejemplos de criterios e indicadores (el Servicio debe diseñar sus propios indicadores de acuerdo a su naturaleza y necesidades) que pueden establecerse en relación al análisis de la información derivada de la Matriz de Riesgos Estratégica del Servicio, se muestran, a continuación en el cuadro Nº 17.

Cuadro Nº 17: Ejemplos de criterios e indicadores para análisis de la información

Criterio	Posibles indicadores para análisis	Responsable	Plazos
Severidad del Riesgo	• Procesos con más altas severidades del riesgo. • Subprocesos con más altas severidades de riesgo. • Etapas con más altas severidades de riesgo, etc.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Exposición al Riesgo	• Procesos con más altas exposiciones al riesgo. • Subprocesos con más altas exposiciones al riesgo. • Etapas con más altas exposiciones al riesgo, etc.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Impacto al Riesgo	• Procesos con riesgos de impactos más altos. • Subprocesos con riesgos de impactos más altos. • Etapas con riesgos de impactos más altos, etc.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.
Tipos de Riesgos	• Tipologías de Riesgos que más se repiten. • Tipos de riesgos con mayor exposición. • Tipos de riesgos con mayor impacto, etc.	Encargado de Riesgos en conjunto con los coordinadores de riesgos.	En el mes de enero de cada año.

Controles	• Procesos con controles más efectivos. • Procesos con controles menos efectivos. • Riesgos extremos con controles menos efectivos, etc.	Encargado de Riesgos en conjunto con los coordinadores de riesgos	En el mes de enero de cada año.
Ranking	• Procesos en los primeros lugares del ranking y su relación al negocio. • Procesos en los primeros lugares del ranking y su relación al soporte. • Procesos priorizados y profundidad del levantamiento realizado, etc.	Encargado de Riesgos en conjunto con los coordinadores de riesgos	En el mes de enero de cada año

VIII.- MEJORAS A INCORPORAR EN EL PROCESO DE GESTIÓN DE RIESGOS PARA EL AÑO 2009

La revisión de la documentación relacionada con el Proceso de Gestión de Riesgos por parte del Consejo de Auditoría, ha detectado algunas deficiencias, que sin ser taxativas ni excluyentes, deberían considerarse en la revisión y el mejoramiento del Proceso de Gestión de Riesgos de cada Servicio:

- Pobre desagregación de los procesos en subprocesos y éstos en etapas y riesgos.
- Deficiencias en la justificación de las ponderaciones a nivel de proceso y subproceso (se hace una descripción del proceso o subproceso más que fundamentar la justificación en criterios objetivos).
- Pobre definición de los objetivos operativos, que no siempre contienen un detalle adecuado que de cuenta de la finalidad de la etapa.
- Falta de identificación de algunos riesgos asociados a la etapa.
- Deficiente definición de riesgos que no siempre pueden asociarse a los objetivos operativos.
- Deficiente calificación de los riesgos en relación a la fuente y la tipología, clasificación en dos o más fuentes de riesgos o tipología.
- Falta de coherencia de la severidad de los riesgos, entendiéndose por ello que los procesos que aparecen con alta relevancia en el Servicio tienen impactos bajos.
- Pobre identificación de los riesgos relacionados con el Gobierno Electrónico. En general hay una baja identificación de los nuevos riesgos asociados a los procesos mejorados con TIC en el Servicio.
- Deficiencias en la identificación de controles, ya que de la descripción que se hace en la matriz no aparece que estén orientados a mitigar el riesgo al que se asocian.
- Los controles no se definen en términos de quién los ejecuta, qué actividades realiza, cómo las ejecuta y en qué oportunidad.
- Debilidad en la descripción de los controles, ya que de su definición no es posible deducir que cumpla con los requisitos de diseño de los mismos. (oportunidad, periodicidad, automatización)
- Falta de coherencia en la exposición al riesgo de los procesos, entendiéndose por ello, que los procesos que la Matriz de Riesgos arroja con mayor exposición no son los procesos que presentan las situaciones de mayor criticidad.
- Confusiones conceptuales al escoger la estrategia genérica a utilizar. Esto se produce cuando se escogen estrategias como “aceptar” y se definen acciones que importan “reducir” o “compartir”.

- Falta de coherencia entre la estrategia y las acciones. Esto implica que no siempre se detallan acciones o actividades que se orienten a concretar las estrategias.
- falta de coherencia entre las acciones de tratamiento y el riesgo que pretenden tratar. Las acciones detalladas, no siempre dicen relación con el riesgo al que pretenden mitigar, en efecto, se describen acciones pero estas no están orientadas a afectar el riesgo al cual se asocian, y no aparece claro cómo esas acciones pueden evitar, compartir o reducir efectivamente el riesgo al cual se asocian.
- Errores y confusiones conceptuales acerca del sentido y utilidad de un indicador. En efecto, muchas veces se señalan como indicadores, elementos que no cumplen con los requisitos de tales. En términos conceptuales un indicador es la magnitud utilizada para medir o comparar los resultados efectivamente obtenidos, en la ejecución de un proyecto, programa o actividad. Es el resultado cuantitativo de comparar dos variables.
- Falta de utilidad de los indicadores. Los indicadores no sirven para medir el grado de implementación de la estrategia, lo que no permiten evaluar el cambio que produce en el riesgo a tratar la aplicación de la estrategia específica.
- Falta de consistencia entre las metas y el indicador, ya que no siempre reflejan el logro que se persigue o el objetivo a alcanzar al implementar la estrategia.
- Falta de certeza en el verificador. No siempre los verificadores son útiles para dar cuenta del cumplimiento de la meta, sino que describen acciones específicas del Servicio de instrucción o información de determinadas materias.

Estas observaciones generales, en conjunto con el resultado de la auditoría de aseguramiento que realizará el Auditor Interno de cada Servicio, son la base para la revisión y mejoramiento del Proceso de Gestión de Riesgos implementado en la entidad para el año 2009.

IX.- RESUMEN DE REQUERIMIENTOS ESPECÍFICOS PARA EL OBJETIVO GUBERNAMENTAL DE AUDITORÍA 2009/PRIMER TRIMESTRE DEL AÑO 2010 – Nº 3

A continuación, se resumen las actividades que se deben realizar los Servicios, para cada fase del Proceso de Gestión de Riesgos, con la finalidad de dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 - Nº 3.

1.- FASE ESTABLECIMIENTO DEL CONTEXTO

1.1.- Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 - Nº 3

a.- Consideraciones

o **Política y Filosofía de Riesgos:** Formular y aprobar la Política y Filosofía de Gestión de Riesgos de la organización, en anexo Nº 1 se presenta un ejemplo. Debe ser aprobada por resolución de la Jefatura Superior del Servicio.

El Servicio debe analizar si la Política y Filosofía de Riesgos es adecuada y responde a la realidad del Servicio. En esta caso, bastará el envío de un oficio al Consejo de Auditoría al 30.06.09 señalando que se mantiene la Política de Riesgos, en caso contrario, deberá enviarse la resolución que aprueba la modificación de dicha política.

- **Enfoque de análisis:** Para efectos del cumplimiento del Objetivo Gubernamental de Auditoría se continuará con un enfoque de procesos de negocio y procesos de soporte.

- **Cobertura del contexto:** La cobertura en la aplicación del enfoque será el levantamiento a nivel de procesos de todos los relacionados al negocio y soporte del Servicio (100%).

- **Definir roles y responsables:** La dirección debe nombrar responsables del proceso de Gestión de los Riesgos y definir sus funciones. (Al Auditor Interno del Servicio no se le debe asignar esa responsabilidad). En anexo Nº 2 se presenta un ejemplo ilustrativo.

  El Servicio deben examinar la resolución de roles aprobada el año 2007 o modificada en el año 2008, si después de ese análisis, se estima que la actual definición de roles que se contiene en la resolución respectiva, responde a los requerimientos del Proceso de Gestión de Riesgo y que durante la implantación del citado proceso, estos roles funcionaron de forma adecuada, bastará que se remita un oficio al Consejo de Auditoría, al 30 de junio de 2009, señalando que la resolución que define los roles, que fuera emitida durante el año 2007 o durante el año 2008, no tiene modificaciones.

  Si por el contrario, posteriormente al análisis realizado en base al presente Documento Técnico, el Servicio estima que la definición de roles que actualmente posee, no responde a las necesidades del Proceso de Gestión de Riesgos o no ha funcionado en forma adecuada, esta resolución deberá modificarse, remitiendo la correspondiente modificación al Consejo de Auditoría al 30 de junio del año 2009.

b.- Productos solicitados

- Oficio que señale que la resolución de asignación de roles no presenta modificaciones. En el caso que la asignación de roles y responsabilidades hubiere sufrido modificaciones, se debe remitir al Consejo de Auditoría la Resolución que aprueba dicha modificación.

- Oficio que señale que la política de Gestión de Riesgos no presenta modificaciones. En el caso que se hubiera modificado la resolución que aprueba la política de Gestión de Riesgos, remitir la Resolución que aprueba dicha modificación.

2.- FASE IDENTIFICACIÓN DE RIESGOS

2.1.- Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 - Nº 3

a.- Consideraciones

Esta fase se cumple con el levantamiento de información a nivel de los procesos de negocio y soporte (100%), su desagregación en subprocesos, etapas y actividades, para finalmente identificar los riesgos que afectan los objetivos de las etapas de cada proceso.

Para el Objetivo Gubernamental 2009 / Primer Trimestre 2010 – Nº 3, se debe revisar el levantamiento de información de todos (100%) los procesos de negocio y soporte, su desagregación en subprocesos, etapas y actividades, para finalmente identificar los riesgos que afectan los objetivos de las etapas de cada proceso y los controles asociados.

b.- Productos solicitados

- Revisión de la segregación a nivel de subprocesos y etapas, en relación a su adecuación a la realidad del Servicio. Este producto se debe incluir en la Matriz de Riesgos, en la fase "Analizar los Riesgos".

- Revisión de la identificación de procesos del Servicio en la categoría de procesos transversales, de acuerdo al cuadro Nº 1 del presente documento técnico. Este producto se debe incluir en la Matriz de Riesgos, en la fase "Analizar los Riesgos".

- Revisión de la identificación de riesgos de acuerdo a la tipología de riesgos establecida en el cuadro Nº 5 de este documento técnico. El Servicio deberá examinar la clasificación de los riesgos que identifique de acuerdo a los tipos de riesgos de origen interno o externo señalados precedentemente. Este producto se debe incluir en la Matriz de Riesgos, en la fase "Analizar los Riesgos".

- Revisión de la identificación de procesos y riesgos relativos al Gobierno Electrónico. El Servicio deberá revisar y mejorar la identificación de todos los riesgos relacionados con los procesos de Gobierno Electrónico y los controles que existan para ellos. (Revisar sugerencias en anexo Nº 8 del presente Documento Técnico). Este producto se debe incluir en la Matriz de Riesgos, en la fase Analizar los Riesgos.

3.- FASE ANÁLISIS DE RIESGOS

3.1.- Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009 / Primer Trimestre 2010 - Nº 3

a.- Consideraciones

Esta fase se cumple con la construcción de la Matriz de Riesgos Estratégica actualizada, incorporando los conceptos de tipología de riesgos, procesos transversales y de ponderación estratégica por proceso y subproceso, que contiene la valuación de los riesgos, controles y la determinación del nivel de exposición al riesgo en base a las categorías definidas en las escalas de clasificación definidas por el Consejo de Auditoría.

Para cumplir el Objetivo Gubernamental 2009/Primer Trimestre año 2010 – Nº 3, debe actualizarse la Matriz de Riesgos Estratégica, incorporando todas las mejoras derivadas de la revisión de la Matriz del año anterior, y, especialmente incorporando todas las observaciones y sugerencias del Auditor Interno contenidas en el informe de aseguramiento del Proceso de Gestión de Riesgos.

b.- Productos solicitados

o Revisión y mejoramiento de la justificación de la Ponderación estratégica por proceso y subproceso, en base a formato del Cuadro Nº 4 de este documento técnico.

o Matriz de Riesgos Estratégica actualizada, según formato dispuesto en anexo Nº 11 del presente documento y que será enviado en formato Excel a los Servicios, la cual debe ser

validada y remitida por medio de la Aplicación informática que para tal efecto disponga el Consejo de Auditoría.

4.- FASE EVALUACIÓN DE RIESGOS

4.1.- Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 – Nº 3

a.- Consideraciones

La organización debe construir un ranking de riesgos en base a procesos con mayor exposición al riesgo ponderado, y dentro de éstos, por subprocesos, también por exposición al riesgo ponderado, de acuerdo al procedimiento dispuesto en los cuadros Nº 11 y 12 de este Documento Técnico.

En base al análisis de los rankings, deben definirse las prioridades para tratar los riesgos para mantener el nivel de exposición al riesgo dentro del nivel del riesgo aceptado.

Para el año 2009, la organización debe revisar el ranking de riesgos que realizó el año 2008, en base a procesos con mayor exposición al riesgo ponderado, y dentro de éstos, por subprocesos, también por exposición al riesgo ponderado, de acuerdo al procedimiento dispuesto en los cuadros Nº 11 y 12 de este documento técnico.

b.- Productos solicitados

- Ranking de riesgos por procesos de acuerdo al formato definido en el Cuadro 11 de este documento.

- Ranking de riesgos por subprocesos de acuerdo al formato definido en el Cuadro 12 de este documento.

En base al ajuste que pudieran sufrir los rankings, en relación al año anterior, deberá determinarse las prioridades para tratar los riesgos para mantener el nivel de exposición al riesgo dentro del nivel del riesgo aceptado.

5. FASE TRATAMIENTO DE RIESGOS

5.1.- Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 - Nº 3

a.- Consideraciones

El Servicio deberá una vez evaluados y priorizados los riesgos en base a su nivel de exposición al riesgo ponderado, comprometer estrategias para aquellos que tratará, señalando las medidas que se adoptarán para la gestión de esos riesgos.

Para el Objetivo Gubernamental 2009/Primer Trimestre 2010 - Nº 3, el Servicio deberá confeccionar un Plan de Tratamiento de acuerdo a las prioridades que deriven de los rankings en

base a su nivel de exposición al riesgo ponderado, y comprometer estrategias para aquellos riesgos que tratará, señalando las medidas que se adoptarán para la gestión de esos riesgos. Para ello, el Plan de Tratamiento debe contener estrategias, acciones, indicadores y metas que se orienten a obtener que el riesgo a tratar sea efectivamente mitigado, a través del manejo de su probabilidad e impacto o mediante el mejoramiento de los controles asociados.

b.- Productos solicitados

Plan de Tratamiento de Riesgos. Este Plan debe presentarse al 30 de octubre del año 2009, utilizando el formato definido en el cuadro Nº 15 de este documento.

6.- FASE MONITOREO Y REVISIÓN

Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 - Nº 3

a.- Consideraciones

Deben establecerse estructuras de reportes y mantener su registro. Esto implica obtener información relevante, en forma oportuna y periódica sobre el estado de los riesgos en cualquier etapa del proceso con la finalidad de reportar a la dirección oportunamente.

Para el cumplimiento del Objetivo Gubernamental Nº 3 se debe realizar el monitoreo al Plan de Tratamiento, de acuerdo a los plazos establecidos en el Plan presentado al 30.10.08.

b.- Productos solicitados

- Reporte del monitoreo y revisión de aquellos elementos del Plan de Tratamiento que hayan tenido establecido fechas de revisión en el año 2009. Para ello el plazo es el 31.12.09 y se debe utilizar el cuadro Nº 16 de este documento.

7.- FASE COMUNICACIÓN Y CONSULTAS

Consideraciones y productos requeridos para dar cumplimiento al Objetivo Gubernamental de Auditoría 2009/Primer Trimestre 2010 – Nº 3

a.- Consideraciones

En relación con esta fase se solicitará el análisis y mejoramiento de la propuesta de comunicación y consulta entregadas el 2008. También puede acompañarse las mejoras en la propuesta presentada al 30.10.08, que se sugieran en la auditoría de aseguramiento realizada por el Auditor Interno del Servicio. Este informe se acompañará al 30.11.09.

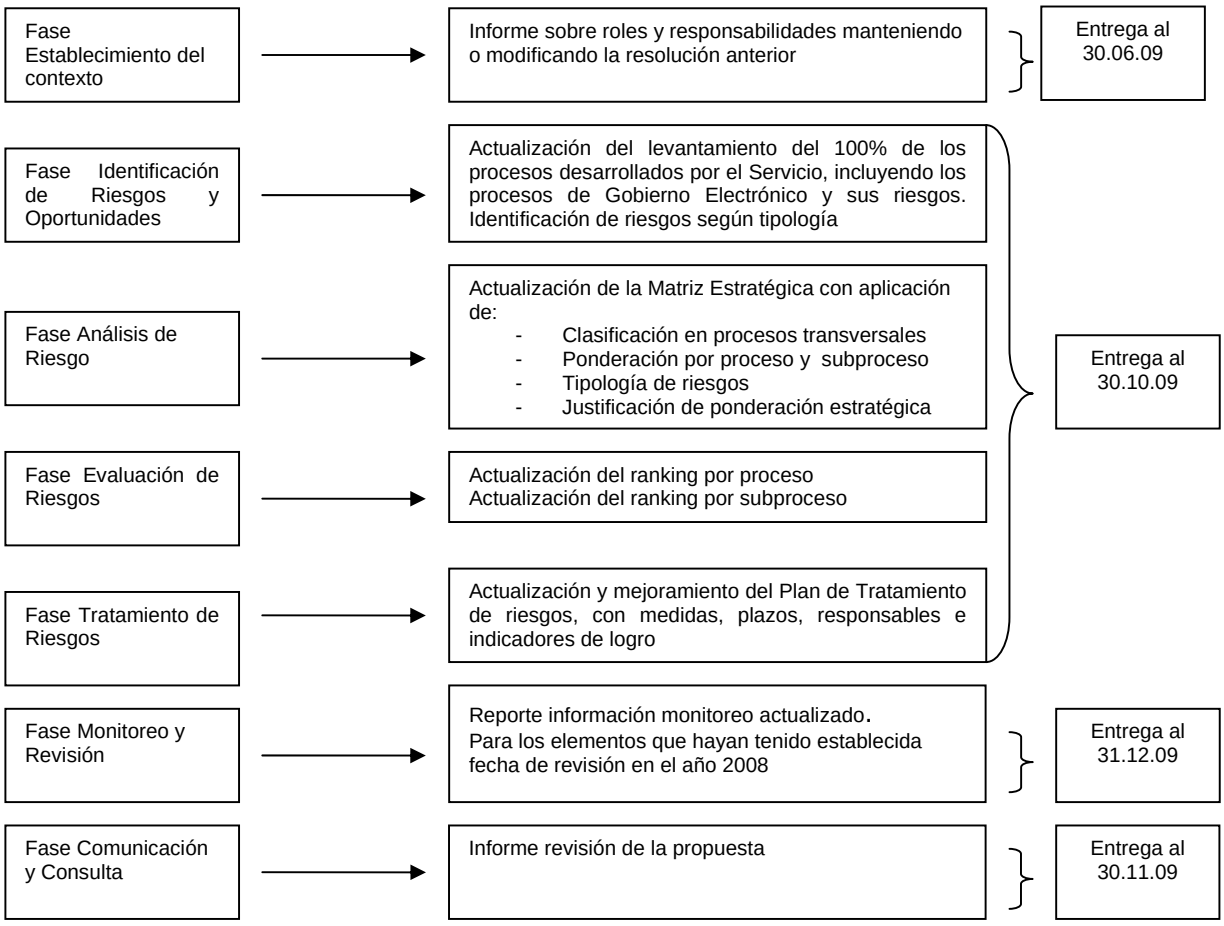
b.- Productos solicitados

- Revisión del sistema de comunicación y consulta, actualización y mejora. Este sistema de comunicación y consulta, debe contener a lo menos los siguientes antecedentes:

    - Qué tipo de información se espera recopilar en el proceso.

- Cuándo se recogería la información, periodicidad.
- Qué tipo de instrumentos recogerán esa información.
- Qué tipo de reportes podría tener el proceso.
- Qué tipo de análisis podrían contener los reportes.
- Qué información se contendría en los instrumentos y el soporte, con que cobertura y amplitud.
- Roles y responsables de la calidad y confiabilidad de la información.
- Sistemas involucrados en el manejo de información del proceso de Gestión de Riesgos al interior del Servicio, soportes y sistemas.
- Niveles organizacionales y personas a quienes se comunicará la información, diferencia de comunicación por acceso.
- Cómo se realizará la comunicación, identificar los soportes y tecnologías requeridas.
- Cuándo se realizará la comunicación de la información, indicar periodicidad.
- Cómo y quiénes tendrán acceso a la comunicación, señalar los criterios para definir perfiles por tipo de información.
- Cómo se recolectarán opiniones que genere la comunicación, espacios de participación, forma como se hará efectiva la participación.
- Señalar roles y responsables de la comunicación y la participación.

8.- FLUJOGRAMA DE TODAS LAS FASES DEL PROCESO DE GESTIÓN DE RIESGOS Y REQUERIMIENTOS ESPECÍFICOS PARA DAR CUMPLIMIENTO AL OBJETIVO GUBERNAMENTAL DE AUDITORÍA 2009/Primer Trimestre 2010 - Nº 3



8.1.- Plazos de entrega de informes y productos solicitados

- Como se observa del flujograma precedente, el cumplimiento del Objetivo Gubernamental 2009/Primer Trimestre 2010 - Nº 3, se realizará por parcialidades.
- Los productos de la fase 1 se entregarán al 30 de junio del año 2009. Los productos de las fases 2, 3, 4, 5 serán entregados al Consejo de Auditoría al 30 de octubre del año 2009.
- Los productos de la fase 7 serán entregados al Consejo de Auditoría el 30.11.2009.
- Los productos de la fase 6 serán entregados al Consejo de Auditoría al 31 de diciembre del año 2009.

8.2.- Formatos exigidos - Planillas u otros

Los formatos exigidos para envío de la información, son aquellos que el documento contiene, esto es:

- Cuadro Nº 4 en página 19.
- Cuadro Nº 11 en página 30.
- Cuadro Nº 12 en página 31.
- Cuadro Nº 15 en página 42.
- Cuadro Nº 16 en página 43.

Además deberá remitirse la Matriz de Riesgos Estratégica que se establece en el anexo Nº 11 a través de la Aplicación informática que el Consejo de Auditoría disponga para tal efecto, y, los cuadros antes indicados en planillas construidas en MS Excel en un CD, u otra forma que el Consejo de Auditoría disponga, respetando el formato entregado por este organismo.

Este año, al igual que el anterior, la Matriz de Riesgos Estratégica debe trabajarse en la planilla Excel entregada por el Consejo de Auditoría línea a línea, ello implica que deberán repetirse los conceptos y no utilizarse celdas combinadas. Esta planilla una vez completa deberá validarse en la Aplicación informática que para tal efecto disponga el Consejo de Auditoría.

8.3.- Forma de Envío

La Matriz de Riesgos Estratégica validada a través de la aplicación informática dispuesta por el Consejo de Auditoría, deberá remitirse a este organismo a través de un correo electrónico creado al efecto, u otra forma que el Consejo de Auditoría disponga. Los demás cuadros deben remitirse en formato electrónico en un CD, u otra forma que el Consejo de Auditoría disponga.

IX.- BIBLIOGRAFÍA

- Alfredo Hierro Cuenca. *La Auditoría Interna y las ISO 9000.* Madrid – España: Instituto de Auditores Internos de España, 1988.
- American Institute of Certified Public Accountants (AICPA), Declaraciones *sobre Normas de Auditoría*, versión 1997, traducción Instituto Mexicano de Contadores Públicos, A.C.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 23 - Programa marco para identificar y sistematizar áreas y procesos críticos, construyendo al efecto, mapas de riesgo ministeriales e institucionales,* Santiago de Chile, 2004.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 24 - Programación en Base a Riesgos,* Santiago de Chile, 2005.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 25 - Informe de Auditoría,* Santiago de Chile, 2005.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 26 - Seguimientos en Auditoría,* Santiago de Chile, 2005.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 31 - Ejecución de Auditoría,* Santiago de Chile, 2005.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 33 – Planificación General en Auditoría,* Santiago de Chile, 2006.
- Consejo de Auditoría Interna General de Gobierno, *Documento Técnico Nº 36 – Planificación General en Auditoría,* Santiago de Chile, 2007.
- Esmond C., Gilbert M.; et al., *Electronic Audit Evidence*, Toronto Canadá: Canadian Institute of Chartered Accountants CICA, 2003.
- Franklin F, Enrique Benjamín, Auditoría *Administrativa*, México: Mc Graw Hill, 2001.
- Hevia Vásquez, Eduardo. *Concepto Moderno de la Auditoría*. Madrid – España: Instituto de Auditores Internos de España, 1999.
- Instituto Nacional de Normalización, *NCh-ISO19011.Of2003 - Directrices para la Auditoría de Sistemas de Gestión De la Calidad y/Ambiental*, Santiago de Chile, 2003.
- Sponsoring Organizations of the Treadway Commission (COSO), *Gestión de Riesgos Corporativos, Marco integrado – Resumen Ejecutivo Marco*, España, 2004.
- U.S. General Accounting Office, “Generally Accepted Governamental Auditing Standards”, versión 1994, traducción Contraloría General de la República del Perú.

ANEXO Nº 1

EJEMPLO ILUSTRATIVO DE POLÍTICA DE RIESGOS

La gestión de riesgos proporciona a nuestro Servicio la capacidad para identificar, evaluar y gestionar todo el espectro de riesgos y posibilitar que todo el personal mejore su comprensión del riesgo, lo que permite obtener:

- aceptación responsable del riesgo.
- apoyo a la dirección.
- mejoras en los resultados.
- responsabilidad reforzada.
- liderazgo superior.

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

Como elementos importantes en la Gestión de Riesgos se considerarán:

- La integridad y consistencia de los procedimientos administrativos y procesos asociados.
- La calidad de la gestión de los recursos humanos a través, fundamentalmente, de sus habilidades, perfiles y entrenamiento.
- La infraestructura, y
- La pertinencia, oportunidad y seguridad de la información.

Prevalecerá el enfoque PREVENTIVO y PROACTIVO.

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

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

Nuestra Misión como Servicio consiste en entregar apoyo a la mujer microempresaria, entregándole soporte a la mujer emprendedora con instrumentos de fomento, créditos flexibles y capacitación para los negocios. Lo anterior implica importantes riesgos pero también oportunidades. Por una parte, la mujer ha tomado un papel de importancia en la sociedad y ha escalado posiciones de poder y empresariales de relevancia. Además, la mujer en general, es puntual en el pago de sus obligaciones y en el cumplimiento de sus compromisos. Sin embargo, también surgen riesgos relacionados con la vulnerabilidad del sector al que está orientado el

Servicio, ya que se trata de mujeres de bajos ingresos y nivel cultural. Además la expansión del comercio electrónico obliga a capacitar a nuestras usuarias en el uso y manejo de las tecnologías que les permitan insertarse en el mundo de los negocios.

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

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

En el marco del proceso de Gestión de Riesgos, la Dirección Ejecutiva utilizará la metodología del Consejo de Auditoria esto es, se levantarán estos procesos, desagregándose por subproceso, etapas, actividades y riesgos y priorizará los procesos y subprocesos en función de la importancia relativa de cada uno de ellos en el cumplimiento de la misión institucional y objetivos estratégicos, para luego ser administrados, utilizando alguna de las siguientes estrategias genéricas, adecuadas a la realidad del Servicio:

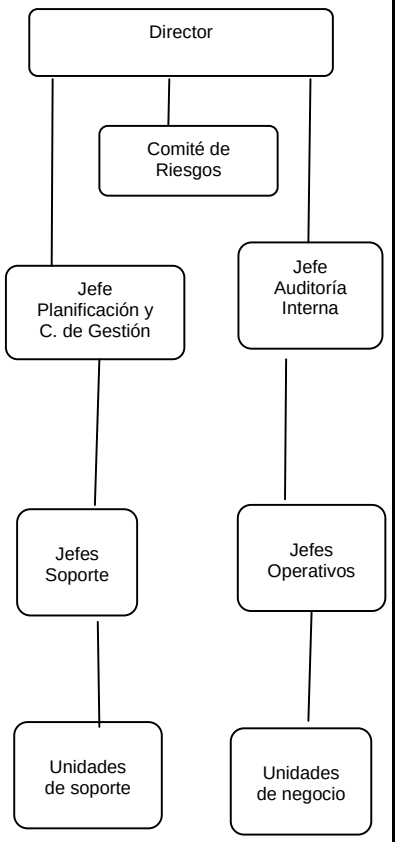
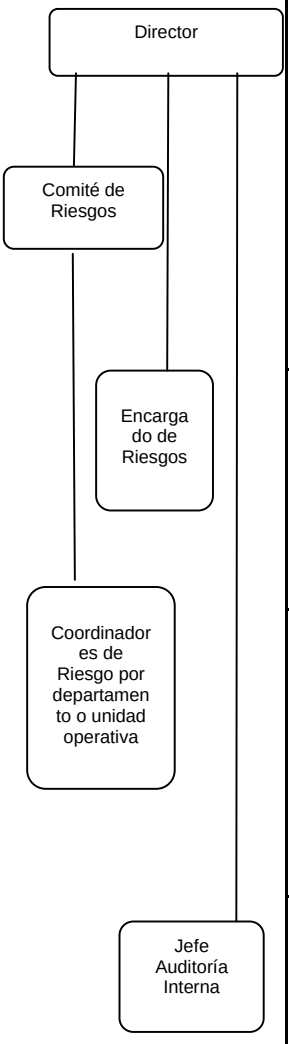
- Evitar
- Compartir
- Reducir
- Aceptar

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

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

ANEXO Nº 2

EJEMPLO DE DEFINICIÓN DE ROLES

Ejemplo de Estructura organizacional	Responsabilidades de administración de riesgos	Ejemplo de Roles claves	Ejemplo de Tareas
		Rol supervisor Coordinar decisión	**Director:** Aprobación políticas escritas Evaluar efectividad esquema de administración riesgos **Comité de Riesgos:** Supervisar implementación del marco de administración de riesgos y su revisión Monitorear perfil riesgo de la organización Asegurarse que los riesgos han sido considerado en planes de largo plazo
		Comprensión del riesgo	**Encargado de Riesgo**: Definir prioridades de riesgo Arbitrar y resolver conflictos Alinear respuesta al riesgo a todas las estrategias de la organización y objetivos del negocio Monitorear el avance general de la implementación de las estrategias de tratamiento
		Operación y soporte. Administrar y reportar riesgos a nivel de negocio	**Coordinadores de Riesgo:** Alinear a través de la organización las prioridades y estrategias de identificación de riesgos Medición de impacto de los riesgos Formular respuestas apropiadas al riesgo Mejora continua de mediciones y procesos Monitorear el avance en su área de la implementación de las estrategias de tratamiento
		Revisión cumplimiento riesgos específicos	**Auditor Interno:** Revisión cumplimiento de riesgos específicos, fraude, oportunidad de negocio, seguros Reporte al Director

		Recolectar, analizar y reportar riesgos y respuestas a los riesgos en la Institución. Cumplimiento en forma independiente y a través de auditoría interna	**Auditoría Interna:** Comunicar y reforzar políticas medición y monitoreo. Revisión de cumplimiento Revisión de cumplimiento del monitoreo Reportes al Director

ANEXO Nº 3

ROL DE LA AUDITORÍA INTERNA EN EL PROCESO DE GESTIÓN DE RIESGOS EN EL SECTOR GUBERNAMENTAL

Cuando nos encontramos en una entidad gubernamental que cuenta con un Proceso de Gestión de Riesgos en operación; la formulación de Matriz de Riesgos y las estrategias para tratar y monitorear los riesgos pasan a ser parte de los elementos que la auditoría interna siempre debe considerar en su planificación y programación.

Por lo tanto, en base a normas de auditoría y en la experiencia que se ha obtenido en el levantamiento de riesgos en el Sector Gubernamental, se puede concluir que el rol fundamental de la auditoría interna en el Proceso de Gestión de Riesgos será proveer aseguramiento objetivo a la dirección sobre la efectividad de las actividades del proceso de gestión de riesgos para ayudar a asegurar que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente.

En las organizaciones se debe comprender que la Jefatura Superior siempre mantiene la responsabilidad de la gestión de riesgo y que los auditores internos deben proveer asesoría, y motivar las decisiones gerenciales sobre riesgos, y no tomar decisiones sobre gestión de riesgo.

Estas directrices deben afectar en forma gradual el enfoque y las orientaciones con las que en la actualidad se definen las actividades de auditoría:

1.- Roles para la auditoría interna en el Proceso de Gestión de Riesgos en el Sector Gubernamental

Los principales factores que los auditores internos deben tomar en cuenta cuando determinen el rol de auditoría interna son si la actividad representa alguna amenaza sobre la independencia y objetividad al realizar su trabajo, y si podría mejorar los Procesos de Gestión de Riesgo y el control interno en la organización.

1.1.- Principales Roles recomendados en el Proceso de Gestión de Riesgos en el Sector Gubernamental

- Realizar evaluación y entregar aseguramiento sobre el Proceso de Gestión de Riesgo a la dirección.
- Brindar aseguramiento de que los riesgos son correctamente evaluados en el Proceso de Gestión de Riesgos.
- Revisión del manejo y evaluación de reportes de riesgos claves.

1.2.- Algunos Roles que deben realizarse con independencia y objetividad en el Proceso de Gestión de Riesgos en el Sector Gubernamental

- Facilitación, identificación y evaluación de riesgos.
- Entrenamiento a la alta dirección sobre respuesta a riesgos.
- Coordinación de actividades del Proceso de Gestión de Riesgos.

- Mantenimiento y desarrollo del marco del Proceso de Gestión de Riesgos.

- Defender el establecimiento del Proceso de Gestión de Riesgos.
- Desarrollo de estrategias de gestión de riesgo para aprobación de Jefatura del Servicio.

2.- Algunos Roles que auditoría interna NO deben realizar en el Proceso de Gestión de Riesgos en el Sector Gubernamental

- Establecer el nivel de Riesgo Aceptado.
- Imponer Procesos de Gestión de Riesgo.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos.
- Tener roles y responsabilidad de la gestión de los riesgos.

ANEXO Nº 4

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

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

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

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

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

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

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

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

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

- El tipo de proceso; estratégico o de soporte.

- Él o los responsables de la gestión.

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

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

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

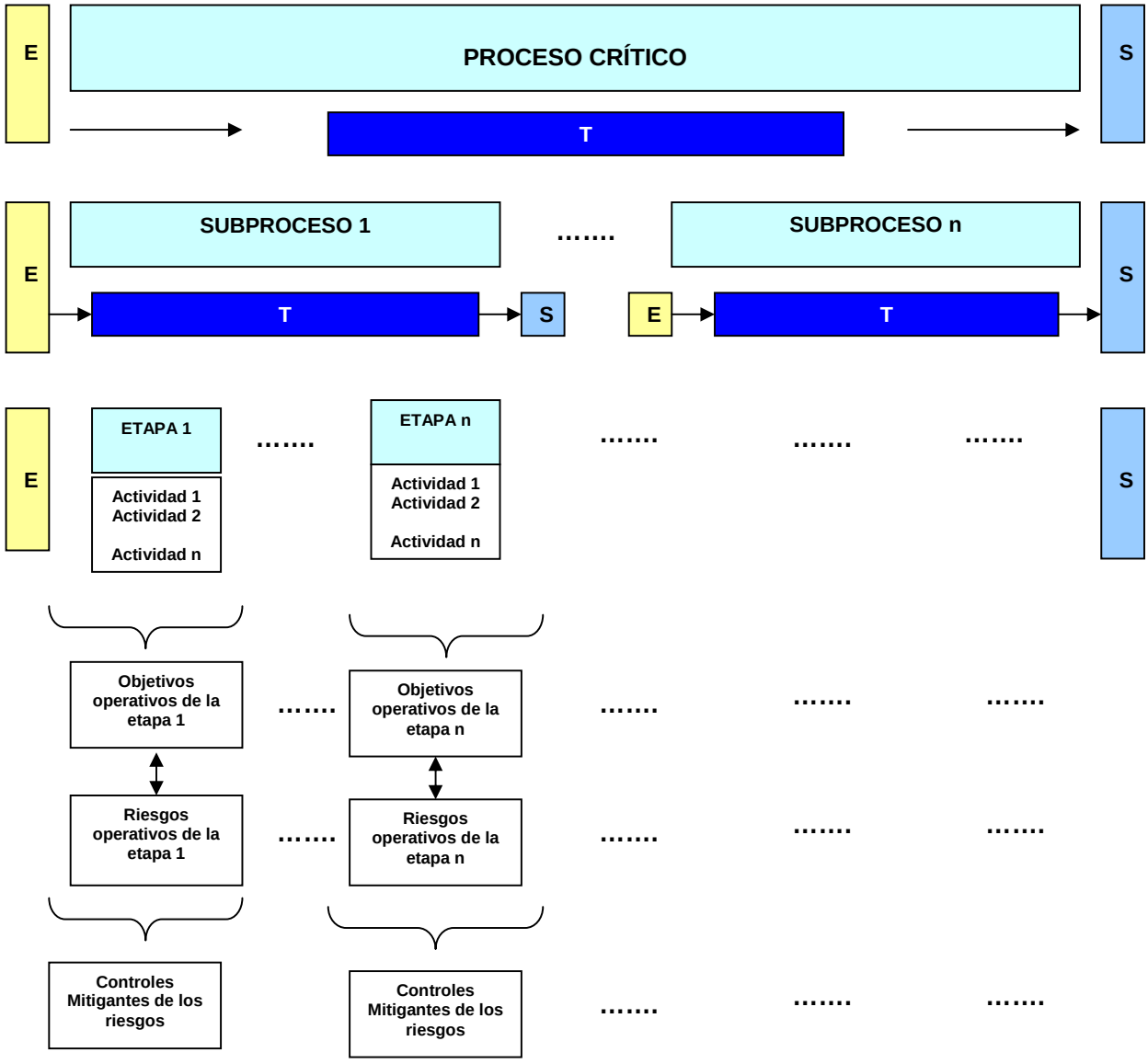
Para efecto de este análisis, las actividades desarrolladas en la etapa también consideran en forma implícita las tareas necesarias para producir y controlar las salidas del subproceso o proceso.

Este tipo de análisis tiene como principal finalidad, identificar donde se encuentran, al mayor nivel de detalle posible, en un determinado proceso, los puntos críticos que deben

ser evaluados y controlados, respecto del nivel de severidad y/o exposición que presentan los riesgos que se han identificado en el estudio realizado.

Para efecto de una mejor comprensión de lo previamente señalado, se presenta un esquema explicativo en el cuadro Nº 1:

Cuadro Nº 1. Esquema de desagregación y análisis de procesos críticos



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

T Transformación: tareas, actividades y responsabilidades.

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

ANEXO Nº 5

TABLAS DE VALUACIÓN PARA CONSTRUIR LA MATRIZ DE RIESGOS ESTRATÉGICA

1.- SEVERIDAD DEL RIESGO

1.1.- Cuadro Nº 1. Categorías de probabilidad:

Categoría	Valor	Descripción
Casi certeza	**5**	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente. (90% a 100%).
Probable	**4**	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente.
Moderado	**3**	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente.
Improbable	**2**	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente.
Muy improbable	**1**	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente.

1.2.- Cuadro Nº 2. Categorías de Impacto:

Categoría	Valor	Descripción
Catastróficas	**5**	Riesgo cuya materialización influye gravemente en el desarrollo del proceso y en el cumplimiento de sus objetivos, impidiendo finalmente que éste se desarrolle.
Mayores	**4**	Riesgo cuya materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Moderadas	**3**	Riesgo cuya materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma adecuada.
Menores	**2**	Riesgo que causa un daño menor en el desarrollo del proceso y que no afecta mayormente el cumplimiento de sus objetivos estratégicos.
Insignificantes	**1**	Riesgo que puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afecta el cumplimiento de sus objetivos estratégicos.

1.3.- Cuadro Nº 3. Nivel de Severidad del riesgo

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)
Casi Certeza (5)	Mayores (4)	EXTREMO (20)
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)
Casi Certeza (5)	Menores (2)	ALTO (10)
Casi Certeza (5)	Insignificantes (1)	ALTO (5)
Probable (4)	Catastróficas (5)	EXTREMO (20)
Probable (4)	Mayores (4)	EXTREMO (16)
Probable (4)	Moderadas (3)	ALTO (12)
Probable (4)	Menores (2)	ALTO (8)
Probable (4)	Insignificantes (1)	MODERADO (4)
Moderado (3)	Catastróficas (5)	EXTREMO (15)
Moderado (3)	Mayores (4)	EXTREMO (12)
Moderado (3)	Moderadas (3)	ALTO (9)
Moderado (3)	Menores (2)	MODERADO (6)
Moderado (3)	Insignificantes (1)	BAJO (3)
Improbable (2)	Catastróficas (5)	EXTREMO (10)
Improbable (2)	Mayores (4)	ALTO (8)
Improbable (2)	Moderadas (3)	MODERADO (6)
Improbable (2)	Menores (2)	BAJO (4)
Improbable (2)	Insignificantes (1)	BAJO (2)
muy improbable (1)	Catastróficas (5)	ALTO (5)
muy improbable (1)	Mayores (4)	ALTO (4)
muy improbable (1)	Moderadas (3)	MODERADO (3)
muy improbable (1)	Menores (2)	BAJO (2)
muy improbable (1)	Insignificantes (1)	BAJO (1)

En el cuadro anterior se muestra el resultado de la combinación entre las categorías del nivel de impacto del riesgo y las categorías del nivel de probabilidad de ocurrencia del riesgo, es decir, el nivel de severidad.

De ese esquema se puede observar que las categorías de impacto tienen una mayor incidencia en el nivel de severidad asignado, puesto que aunque la probabilidad de ocurrencia sea menor, al tratarse de riesgos con impactos altos, cualquier materialización del riesgo (aunque sea en sólo una oportunidad) tendrá una consecuencia significativa en el cumplimiento de los objetivos del proceso examinado.

Esto explica los casos en que a igual valor, la severidad del riesgo es distinta. A modo de ejemplo se presentan las siguientes relaciones:

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
muy improbable (1)	Mayores (4)	ALTO (4)
Probable (4)	Insignificantes (1)	MODERADO (4)
Probable (4)	Moderadas (3)	ALTO (12)
Moderado (3)	Mayores (4)	EXTREMO (12)

2.- CLASIFICACIÓN DEL CONTROL CLAVE

2.1.- Diseño del control

- **Cuadro Nº 4. Oportunidad de la acción del control (O):**

Clasificación	Descripción
Preventivo (Pv)	Controles claves que actúan antes o al inicio de una actividad.
Correctivo (Cr)	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias.
Detectivo (Dt)	Controles claves que sólo actúan una vez que el proceso ha terminado.

- **Cuadro Nº 5. Periodicidad en la acción del control (PD):**

Clasificación	Descripción
Permanente (Pe)	Controles claves aplicados durante todo el proceso, es decir, en cada operación.
Periódico (Pd)	Controles claves aplicados en forma constante sólo cuando ha transcurrido un período específico de tiempo.
Ocasional (Oc)	Controles claves que se aplican sólo en forma ocasional en un proceso.

- **Cuadro Nº 6. Automatización en la aplicación del control (A):**

Clasificación	Descripción
100% automatizado (At)	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas informatizados.
Semi – automatizado (Sa)	Controles claves incorporados en el proceso, cuya aplicación es parcialmente desarrollada mediante sistemas informatizados.
Manual (Ma)	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados.

2.2.- Cuadro Nº 7. Escala de clasificación de la efectividad de los controles

CUMPLIMIENTO CON NORMAS O REQUISITOS DE CONTROL	CARACTERÍSTICAS DISEÑO CONTROL CLAVE/FUNDAMENTAL			CLASIFICACIÓN	VALOR DEL DISEÑO DEL CONTROL
	PERIODICIDAD (PD)	OPORTUNIDAD (O)	AUTOMATIZACIÓN (A)		
CUMPLIMIENTO ADECUADO	PERMANENTE	PREVENTIVO	INFORMATIZADO	OPTIMO	5
CUMPLIMIENTO ADECUADO	PERMANENTE	CORRECTIVO	INFORMATIZADO		
CUMPLIMIENTO ADECUADO	PERMANENTE	DETECTIVO	INFORMATIZADO	BUENO	4
CUMPLIMIENTO ADECUADO	PERIODICO	PREVENTIVO	INFORMATIZADO		
CUMPLIMIENTO ADECUADO	PERIODICO	CORRECTIVO	INFORMATIZADO	MAS QUE REGULAR	3
CUMPLIMIENTO ADECUADO	PERIODICO	DETECTIVO	INFORMATIZADO		
CUMPLIMIENTO ADECUADO	OCASIONAL	PREVENTIVO	INFORMATIZADO	REGULAR	2
CUMPLIMIENTO ADECUADO	OCASIONAL	CORRECTIVO	INFORMATIZADO		
CUMPLIMIENTO ADECUADO	OCASIONAL	DETECTIVO	INFORMATIZADO	DEFICIENTE	1
INSUFICIENTE	NO DETERMINADO	NO DETERMINADO	NO DETERMINADO	INEXISTENTE	1

En el esquema anterior se señala que en primer lugar, se debe evaluar si el control mitigante asociado a un riesgo tiene un nivel de cumplimiento adecuado respecto de las normas o requisitos de control básicos que en este modelo se han relevado para dar razonable seguridad de cumplimiento de los objetivos y metas. Esto implica realizar un análisis integral de las referidas normas o requisitos (segregación, autorización, formalización, etc.) y determinar si éstas se cumplen de para un control examinado en particular.

Producto de este análisis, se puede dar que los referidos requisitos se cumplan satisfactoriamente, es decir, que el control esté sustentado en una estructura básica sólida. Posteriormente, se debe seguir con el análisis del diseño del control, este aspecto es relevante, ya que los riesgos son por naturaleza dinámicos y requieren que los controles tengan una estructura que se oriente a la prevención de la materialización del efecto de los riesgos dinámicos.

Finalmente, se debe clasificar el nivel de efectividad del control examinado, de acuerdo con el esquema presentado, asignándole el valor respectivo según la escala.

En caso que esto no ocurra, es decir, los requisitos no presentan un cumplimiento suficiente en el control examinado, debe entenderse que su nivel de cumplimiento es

insuficiente y corresponde clasificarlo como si se tratara de un control inexistente, con valoración de 1, sin que ya sea necesario evaluar la efectividad en el diseño del control respecto de la ocurrencia del riesgo.

Por consiguiente, debe clasificarse como inexistente, con nivel de eficiencia del control examinado de 1, de acuerdo con la escala contenida en el esquema presentado.

Para ver mayores detalles de las normas o requisitos de control básicos considerados en este modelo ver anexo Nº 9.

3.- NIVELES DE CLASIFICACIÓN DEL NIVEL DE EXPOSICIÓN AL RIESGO

La exposición al riesgo está determinada por la severidad del riesgo dividida por la eficiencia del control asociado a ese riesgo. Estos elementos se obtienen de las relaciones detalladas previamente en este anexo.

A continuación se presenta la escala de nivel de exposición al riesgo que los califica:

Cuadro Nº 8. Escala del nivel de exposición al riesgo

INDICADOR DE EXPOSICIÓN AL RIESGO	VALOR	NIVEL DE EXPOSICIÓN AL RIESGO
NIVEL SEVERIDAD DEL RIESGO / NIVEL EFICIENCIA DEL CONTROL	8,0 – 25,0	NO ACEPTABLE (Na)
	4,0 – 7,99	MAYOR (Ma)
	3,0 – 3,99	MEDIA (Md)
	0,2 - 2,99	MENOR (Me)

Tal como se señaló, la escala previamente presentada, ha sido construida en base a la relación entre el nivel de severidad del riesgo (Bajo, Moderado, Alto. Extremo) y el nivel de eficiencia del control asociado a ese riesgo (Deficiente, Regular, Más que regular, Bueno, Óptimo). Dicha relación se presenta en el cuadro Nº 9.

Un primer análisis de dicha escala observaría que los niveles de exposición al riesgo Mayor y No Aceptable, pudiesen tener un rango muy extenso de valores; 4,0 a 7,99 y 8,0 a 25 puntos respectivamente, pero al realizar un análisis más riguroso, se debería observar que en realidad los niveles de exposición al riesgo con valores más altos, corresponden a las combinaciones entre los niveles de riesgo más severos y los niveles de eficiencia del control más Bajos, o a las combinaciones entre los riesgos con severidad más altas y con controles que tienen un nivel de efectividad sólo de Regular.

Por otra parte, los niveles de exposición al riesgo más bajos están conformados por las combinaciones entre los niveles de riesgos menos severas y los niveles de eficiencia del

control más altos, o por las combinaciones entre riesgos con severidades Bajas y controles con niveles de efectividad Deficiente o Regular, o por las combinaciones entre riesgos con severidad altas, pero con controles con nivel de efectividad Óptimo o Bueno.

Por ejemplo, en el esquema Nº 9 se observa que el nivel de exposición al riesgo E1 = 10, (Nivel de exposición al riesgo No Aceptable) está conformado por un nivel de severidad del riesgo, Extremo = 20 y un nivel de efectividad de control, Regular = 2.

En el caso del nivel de exposición E2 = 4 (Nivel de exposición al riesgo Mayor), está conformado por un nivel de severidad del riesgo, Alto = 12 y un nivel de efectividad de control, Más que Regular = 3.

Finalmente, el nivel de exposición E3 = 1 (Nivel de exposición al riesgo Menor), está conformado por un nivel de severidad del riesgo, Alto = 5 y un nivel de efectividad de control, Óptimo = 5.

Esquema Nº 9. Relaciones entre severidad del riesgo y efectividad del control que determinan la escala del nivel de exposición al riesgo

NIVEL DEL RIESGO			NIVEL DE LA EFECTIVIDAD DEL CONTROL				
			OPTIMO	BUENO	MAS QUE REGULAR	REGULAR	DEFICIENTE
			5	4	3	2	1
BAJO - MODERADO - ALTO - EXTREMO	EXTREMO	25	5	6,25	8,33	12,5	25
		20	4	5	6,67	10 E1	20
		16	3,2	4	5,33	8	16
	ALTO	15	3	3,75	5	7,5	15
		12	2,4	3	4 E2	6	12
		10	2	2,5	3,33	5	10
	MODERADO	9	1,8	2,25	3	4,5	9
		8	1,6	2	2,67	4	8
		6	1,2	1,5	2	3	6
		5	1 E3	1,25	1,67	2,5	5
	BAJO	4	0,8	1	1,33	2	4
		3	0,6	0,75	1	1,5	3
		2	0,4	0,5	0,67	1	2
		1	0,2	0,25	0,33	0,5	1

ANEXO Nº 6

EJEMPLO DE LEVANTAMIENTO DE INFORMACIÓN DE UN PROCESO

A continuación se presenta un ejemplo de levantamiento de información del subproceso "Compra de bienes y servicios", que forma parte del proceso crítico denominado "Compras y Abastecimiento" en una entidad ficticia.

Con la finalidad de lograr una mejor comprensión del ejemplo, se hará un análisis detallado de los riesgos y controles para las etapas de Selección y Adjudicación.

1.- Cuadro: Levantamiento de información de cada proceso

Proceso	Subprocesos	Etapas	Entradas del subproceso o proceso	Salidas del subproceso o proceso
De compras y abastecimiento	Planificación operativa anual de compras.	....	....	....
		....	....	....
		....	....	....
	Compra de bienes y servicios.	Definición naturaleza del proceso.	Plan Operativo de compras.	Bienes y servicios (insumos) de calidad que satisfagan los requerimientos para producción del Servicio.
		Confección y publicación de Bases.		
		Selección.		
		Adjudicación.		
	Recepción y evaluación de bienes y servicios adquiridos.	....	....	....
		....	....	....
		....	....	....
	....	....	....	....
	....	....	....	....

2.- Cuadro: Levantamiento de información de las etapas Selección y Adjudicación

Etapas	Objetivo operativo de la etapa	Actividades de la etapa		Responsables
		De gestión	De control	
Etapa Definición de la naturaleza del proceso de compras a utilizar (convenio marco, licitación pública, privada, trato directo).	Definir de acuerdo a las características del bien o servicio a comprar, la forma de adquirirlo en el mercado, de conformidad a la normativa de compras.	1.- El Comité de Compras, en base a lo establecido en el Plan de Compras define cómo se realizará cada adquisición (licitación pública, privada o trato directo).		Comité de Compras
			2.- El Jefe de Finanzas y de la Unidad Jurídica visan la definición del Comité.	Jefe Finanzas Jefe Unidad Jurídica

Etapa Confección y publicación de bases.	Establecer formalmente bases administrativas y técnicas adecuadas a la especificación técnica de lo requerido y que respeten la transparencia e igualdad de los oferentes.	1.- Se realiza la definición de especificaciones técnicas (características, plazos, volúmenes, calidades, etc.).		Encargado de especificaciones técnicas de compras
			2.-Validan y visan la definición técnica.	Jefe de Abastecimiento y Jefe Unidad solicitante
		3.- Confeccionar bases de licitación oportunas y completas (de acuerdo con el procedimiento formal del Servicio).		Jefe de Finanzas Jefe de la Unidad Jurídica
			4.- Aprobación oportuna de las Bases de Licitación.	Jefe de la Unidad Jurídica Jefe de Servicio
		5.- Publicar en diarios en forma completa, oportuna y legal		Jefe de Finanzas
		6.- Aclarar en forma completa e igualitaria las dudas de los oferentes.		Jefe de Finanzas Jefe de la Unidad Jurídica
			7.- Verificación que todas las compras cuenten con una carpeta con antecedentes de licitación, bases y publicación.	Encargado de análisis del área de compras
Etapa Selección	Realizar una selección transparente, garantizando la participación igualitaria de los oferentes.	**Licitaciones privada y pública**		
		1.- Recepción de todas las ofertas remitidas. (igualdad de oferentes)		Comité de Compras
		2.- Apertura de acuerdo a la normativa de compras, a través del sistema de Chilecompras.		Comité de Compras Encargado del Sistema de Compras.
			3.- Participación de Ministro de Fe en la apertura.	Funcionario de la Unidad Jurídica
			4.- Confección de acta de recepción de ofertas, especificando día y hora de las ofertas recibidas.	Encargado Of. de Partes Jefe de Finanzas

			5.- Confección de acta de apertura con todos los participantes que cumplen requisitos.	Comité de Compras Ministro de Fe
			6.- Entrega de reportes del sistema al comité de compras.	Encargado del sistema de compras y supervisor.
		Compra directa		
		1.- Se designan cotizadores al interior del Servicio.		Jefe de Finanzas y Comité de Compras
			2.- Cruces de datos entre funcionarios participantes del proceso de compras y proveedores.	Jefe de Abastecimiento
		3.- Obtención de a los menos tres cotizaciones en el caso de trato directo.		Cotizadores designados.
Etapa Adjudicación	Adjudicar la compra al oferente que presente la oferta más conveniente para el servicio.		1.- Evaluación técnica, de acuerdo a criterios previos y objetivos dispuestos en procedimiento.	Comité de Compras.
		2.- Se levanta un acta de proposición de adjudicación con el fundamento de la decisión según desarrollo del proceso.		Comité de Compras.
			3.- Revisión de la adjudicación para determinar su conformidad al procedimiento y Bases.	Jefe de Abastecimiento
			4.- Revisión de la consistencia y legalidad del proceso.	Jefe de la Unidad Jurídica

			5.- Se verifica que el proveedor adjudicado no tengan inhabilidades respecto de funcionarios del Servicio y cumplan obligaciones laborales.	Jefe de Finanzas. Jefe de Recursos Humanos.
			6.- Visación de la adjudicación	Jefe de la Unidad Jurídica
		7.- Aprobación de Adjudicación		Jefe de Servicio o delegatario.

3.- Cuadro: Ejemplo de identificación de riesgos asociados a las actividades realizadas para lograr los objetivos operativos de las etapas Selección y Adjudicación

Etapa	Objetivo operativo de la etapa	Actividades de la etapa	Riesgos asociados a la realización de las actividades
Etapa…	**…**	**…**	**…**
Etapa…	**…**	**…**	**…**
Etapa Selección	Realizar una selección transparente, garantizando la participación igualitaria de los oferentes.	**Licitaciones privada y pública**	
		1.- Recepción de todas las ofertas remitidas. (Igualdad de oferentes).	Recepción de ofertas fuera de plazo.
			Recepción de ofertas en forma distinta a la señalada en las bases.
		2.- Apertura de acuerdo a la normativa de compras a través del sistema de Chilecompras.	La apertura no se realiza a través del sistema y no se cumple el procedimiento aprobado.
			La apertura se realiza en día y hora distinta al establecido en las bases.
		3.- Participación de Ministro de Fe en la apertura.	Ministro de Fe con incompatibilidades.
		4.- Confección de acta de recepción de ofertas, especificando día y hora de las ofertas recibidas.	En caso de recepción en papel, no se confecciona Acta de recepción o ésta es incompleta o errónea.
		5.- Confección de acta de apertura con todos los participantes que cumplen con lo requisitos.	Las actas se firman posteriormente por las personas que no asisten a la apertura.
		6.- Entrega de reportes del sistema al comité de compras.	No se entregan reportes en forma oportuna o tienen datos erróneos.
		Compra directa	

		1.- Se designan cotizadores al interior del Servicio.	Designación de cotizadores con incompatibilidades.
		2.- Cruces de datos entre funcionarios participantes del proceso de compras y proveedores	No se realizan cruces de datos entre funcionarios y proveedores
			No se cuenta con la información para cruzar datos
		3.- Obtención de a los menos tres cotizaciones en el caso de trato directo.	Falta de tres cotizaciones para trato directo sin fundamento.
			Cotizaciones manejadas para favorecer a un proveedor.
Etapa Adjudicación	Adjudicar la compra al oferente que presente la oferta más conveniente para el Servicio.	1.- Evaluación técnica, de acuerdo a criterios previos y objetivos dispuestos en procedimientos.	Errores en evaluación técnica.
			Adjudicación con criterios distintos a los establecidos en la ley, las bases y los procedimientos.
		2.- Se levanta un acta de proposición de adjudicación con el fundamento de la decisión según desarrollo del proceso.	Adjudicación no es consistente con el proceso de evaluación.
		3.- Revisión de la adjudicación para determinar su conformidad al procedimiento y Bases.	La adjudicación no es consisten con las Bases o con el procedimiento establecido.
		4.- Revisión de la consistencia y legalidad del proceso.	El proceso presenta deficiencias legales de forma o fondo
		5.- Se verifica que el proveedor adjudicado no tenga inhabilidades respecto de funcionarios del Servicio y cumplan obligaciones laborales..	Inexistencia de antecedentes para realizar la verificación
			Funcionarios que realizan verificación no cuentan con las competencias necesarias.
		6.- Visación de Adjudicación.	No se cuenta con todos los antecedentes para visar la operación.
		7.- Aprobación de la adjudicación.	El funcionario que aprueba no tiene la facultades delegadas

4.- Cuadro: Ejemplo de identificación de riesgos asociados a las entradas del subproceso o Proceso

Etapas que afecta	Objetivo operativo de la etapa	Entradas al subproceso o proceso	Riesgos asociados a las entradas del subproceso o proceso
Etapa Selección	Realizar una selección transparente, garantizando la participación igualitaria de los oferentes.	Plan Operativo de Compras.	1.- Deficiencias técnicas en la formulación del Plan. El Plan no representa las necesidades de compra del Servicio. 2.- Falta de aprobación o autorización del Plan. ...

5.- Cuadro: Identificación de controles mitigantes para cada riesgo operativo asociado a las actividades realizadas en las etapas de Selección y Adjudicación

Etapas	Riesgos asociados a la realización de las actividades	Controles operativos mitigantes clave	Responsables
Etapa Selección	**Licitación privada y pública**		
	Recepción de ofertas fuera de plazo.	El sistema de información ADBG, contiene un algoritmo que controla y chequea la hora y la fecha de la apertura.	Encargado Sistema de Información de Compras
		En caso de ofertas no recibidas por el sistema, el encargado de la Oficina de Partes, levanta un acta con individualización de día y hora de las ofertas recibidas, que es visada por el Jefe de Finanzas.	Encargado Oficina de Partes Jefe de Finanzas
	Recepción de ofertas en forma distinta a la señalada en las bases.	El comité de compras controla el proceso de recepción y levanta un Acta de todas las ofertas recibidas, con participación de un Ministro de Fe. El sistema o el encargado (si son extra sistema) mantiene los antecedentes de las consultas y respuestas a los oferentes, con fecha.	Comité de Compras Encargado del Sistema de Compras

	La apertura no se realiza a través del sistema y no se cumple el procedimiento aprobado.	La recepción y apertura de las ofertas deben realizarse a través del portal de Chilecompras. Este procedimiento es verificado diariamente, mediante un reporte que se emite en el área abastecimiento.	Encargado de Sistema de Información y su supervisor.
	La apertura se realiza en día y hora distinta al establecido en las bases.	En el caso de apertura extra sistema, se realiza en dependencias del Servicio con la asistencia de un Ministro de Fe que certifica que el día y hora corresponde a las Bases.	Funcionario de la Unidad Jurídica.
	Ministro de Fe con incompatibilidades.	Sin control	-
	Las actas se firman posteriormente por las personas que no asisten a la apertura.	En el caso de apertura en soporte de papel, existe un Acta que da cuenta de la apertura firmada por la entidad y los oferentes presentes en la apertura, con la asistencia de un Ministro de Fe.	Comité de Compras Ministro de Fe
	No se entregan reportes en forma oportuna o tienen datos erróneos.	La información se visa.	Supervisor Sistema de Información
	Compra directa		
	Designación de cotizadores con incompatibilidades.	Se realiza un cruce de datos de éstos y los proveedores frecuentes del Servicio	Jefe de Finanzas Jefe de Recursos Humanos
	Cotizaciones manejadas para favorecer a proveedor.	Sin control	-
	Falta de tres cotizaciones para trato directo sin fundamento.	Sin control	-
Etapa Adjudicación	Errores en la evaluación técnica.	El Comité de Compras analiza las ofertas a través de los requisitos establecidos en la Ley, las bases y el procedimiento, emitiendo un informe técnico.	Comité de Compras
	Adjudicación con criterios distintos a los establecidos en la ley y las bases.	El jefe de Abastecimiento revisa y pone visto bueno sólo si se cumplen todos los requisitos.	Jefe de Abastecimiento

	Adjudicación no es consistente con el proceso de evaluación.	La Unidad Jurídica da visto bueno a la resolución de adjudicación antes de la firma del Jefe Superior y revisa la consistencia del proceso.	Jefe de la Unidad Jurídica
	Inexistencia de antecedentes para realizar la verificación.	El Jefe de Finanzas es el encargado de mantener y conseguir las herramientas necesarias para realizar los cruces de datos (bases de datos públicas, declaraciones de interés y otros antecedentes) y de capacitar a los funcionarios que realizan esta labor en el manejo de bases de datos y consultas, y en el manejo de la normativa y jurisprudencia administrativa asociadas a temas de probidad.	Jefe de Finanzas Jefe de Recursos Humanos
	Funcionarios que realizan verificación no cuentan con las competencias necesarias.		
	No se cuenta con todos los antecedentes para visar la operación.	Sin control	-
	El funcionario que aprueba no tiene la facultades delegadas	La Unidad Jurídica previa a la aprobación, la visa, revisando los aspectos de forma y fondo y las atribuciones del firmante.	Jefe Unidad Jurídica

6.- Cuadro: Identificación de controles mitigantes para cada riesgo operativo identificado asociado a las entradas del subproceso o proceso

Etapa que afecta	Riesgos asociados a las entradas del subproceso o proceso	Controles operativos mitigantes claves	Responsables
Etapa Selección	1.- Deficiencias técnicas en la formulación del Plan. El Plan no representa las necesidades del Servicio.	Existe información histórica acerca del gasto y adquisiciones del Servicio. Cada Unidad hace llegar a la Comisión de Planificación, al 15 de enero de cada año, un programa operativo anual con los requerimientos y necesidades para el año, calendarizadas y presupuestadas. Existen procedimientos formales con participación de las diversas instancias para definir el Plan (Comisión de Planificación).	Jefe de Finanzas Jefe de Cada Unidad Operativa Jefe de Servicio Comisión de Planificación
	2.- Falta de aprobación o autorización del Plan.	La jefatura máxima revisa el Plan y de acuerdo a los análisis de la Comisión de Planificación aprueba, rechaza o modifica el Plan propuesto.	Jefe de Servicio Comisión de Planificación

ANEXO Nº 7

EJEMPLOS DE TÉCNICAS DE IDENTIFICACIÓN DE EVENTOS GENERADORES DE RIESGOS Y OPORTUNIDADES

La metodología de identificación de riesgos de una entidad puede comprender una combinación de técnicas, junto con herramientas de apoyo. Por ejemplo, la dirección puede usar talleres interactivos de trabajo como parte de dicha metodología, con un monitor que emplee alguna herramienta tecnológica para ayudar a los participantes.

La profundidad, amplitud, calendarización y disciplina en la identificación de eventos generadores de riesgos, varían según las organizaciones. La dirección selecciona técnicas que encajan con su filosofía de gestión de riesgos y asegura que la entidad desarrolla las capacidades necesarias de identificación de eventos y que están operativas las herramientas de apoyo. Por encima de todo, la identificación de eventos necesita ser potente y fiable, ya que forma la base de los componentes de la evaluación de riesgos y de la respuesta a ellos.

Ejemplos de técnicas de identificación de eventos:

Inventarios de eventos: Son relaciones detalladas de acontecimientos potenciales comunes a empresas o instituciones de un sector determinado, o a un proceso o actividades específicas que se da en diversos sectores. Las aplicaciones de software pueden generar relaciones relevantes de eventos genéricos potenciales que generan riesgos, que algunas entidades usan como punto de partida para la identificación de eventos generadores de riesgos. Por ejemplo, una empresa que está acometiendo un proyecto de desarrollo de software, elaborará un inventario que describa eventos genéricos relativos a este tipo de proyectos.

Análisis interno: Puede llevarse a cabo como parte de un proceso rutinario del ciclo de planificación empresarial u organizacional, normalmente mediante reuniones del personal de la unidad de negocios. El análisis interno utiliza a veces la información procedente de grupos de interés de dicha unidad (clientes, proveedores y otras unidades del negocio) o de expertos en el tema ajenos a ella (expertos funcionales internos, externos o la unidad de auditoría interna). Por ejemplo, una empresa u organización que esté considerando introducir un nuevo producto, usa su propia experiencia histórica, junto con investigación externa de mercado que identifique eventos generadores de riesgos que hayan afectado al éxito de productos de los competidores.

Dispositivos de escala o umbral: Estos dispositivos alertan a la dirección respecto a áreas con problemas comparando transacciones o eventos actuales con criterios predefinidos. Una vez que suena la alarma, es posible que un evento generador de riesgo presente una evaluación ulterior o una respuesta inmediata. Por ejemplo, la dirección de una empresa hace un seguimiento del volumen de ventas en mercados seleccionados, con vistas a nuevos programas de marketing o publicidad, y reorienta los recursos según los resultados. La dirección de otra empresa sigue las estructuras de precios de los competidores y contempla cambios en sus propios precios cuando se franquea determinado umbral.

Talleres de trabajo y entrevistas: Estas técnicas identifican los eventos generadores de riesgos aprovechando el conocimiento y la experiencia acumulada de la dirección, el personal y los grupos de interés, a través de discusiones estructuradas. Un monitor lidera y facilita la discusión sobre los eventos que puedan afectar a la consecución de objetivos del Servicio o alguna de sus unidades. Por ejemplo, un controller financiero dirige un taller de trabajo con miembros del equipo contable, para identificar eventos que puedan afectar a los objetivos de información financiera externa. Al combinar los conocimientos y experiencia de los miembros del equipo, se identifican eventos importantes que de otro modo podrían haberse olvidado.

Indicadores de eventos importantes: Supervisando datos correlacionados con los eventos generadores de riesgos, las entidades identifican la existencia de condiciones que podrían dar lugar a un acontecimiento. Por ejemplo, las instituciones financieras reconocen desde hace mucho tiempo la correlación entre la demora del pago de préstamos y su eventual impago futuro, así como el efecto positivo de una intervención anticipada. Por ello, el control de las pautas de pago permite mitigar el impago mediante acciones oportunas anticipadas.

Metodología para datos de eventos con pérdidas: Los archivos de datos sobre eventos individuales con pérdidas en el pasado son una fuente útil de información para identificar las tendencias y causas principales. Una vez que se identifica una de estas, la dirección puede averiguar que es más efectivo, si evaluarla y tratarlo o afrontar los eventos individuales. Por ejemplo, una empresa que explota una gran flota de coches mantiene una base de datos de las reclamaciones por accidentes y, mediante su análisis, averigua que un porcentaje desproporcionado de ellos, tanto en número como en importe, se vincula a conductores del equipo en ciertas unidades, localizaciones geográficas y franjas de edad. Este análisis capacita a la dirección para identificar las causas principales de los eventos y tomar acciones.

ANEXO Nº 8

EJEMPLOS DE RIESGOS Y CONTROLES RELACIONADOS CON EL GOBIERNO ELECTRÓNICO

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

1) Fragilidad de los sistemas de información

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

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

2) Inseguridad de la información

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

- **Riesgos de Integridad:** Este riesgo abarca todos aquellos relacionados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos existen en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en la Interfase del usuario, procesamiento de errores y administración de cambios.

- **Riesgos de usabilidad:** Se refiere a los riesgos relacionados al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

- **Riesgos de acceso:** Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Abarcan los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información.

- **Riesgos de recuperabilidad:** Relacionados con las deficiencias en las técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas y los Backups y planes de contingencia que controlan desastres en el procesamiento de la información, entre otros.

- **Riesgos en la infraestructura:** Estos riesgos se refieren a que en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

- **Riesgos de seguridad general:** Referidos a los Riesgos de choque de eléctrico, riesgos de incendio, de niveles inadecuados de energía eléctrica, de radiaciones, mecánicos, etc.

3) Riesgos relacionados con los documentos electrónicos

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

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

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

cumplimiento de los procedimientos establecidos y la tecnología basada en encriptación de datos, firmas electrónicas y certificados digitales.

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

- **Controles para riesgos de autenticación:** Smart card o tokens, Password, Biometría, PKI Infraestructura de clave pública, certificados digitales, Firewalls, etc.

- **Controles para riesgos de integridad:** Control de acceso a aplicaciones, funciones automáticas que permitan segregación de funciones, validación de datos, reportes de excepciones, controles de secuencia numérica y de coincidencia, control de rastros de correcciones, firma electrónica, firewalls entre otros.

- **Controles para riesgos de no repudio:** Técnicas criptográficas, certificados digitales, firma electrónica avanzada, time stamping, entre otros.

- **Controles para riesgos de autorización:** Controles de acceso, definición de perfiles de usuario en redes, aplicaciones y sistemas; firma electrónica, certificados digitales, etc.

- **Controles para riesgos de disponibilidad:** Controles asociados a la adquisición, desarrollo y mantenimiento de sistemas, mecanismos de recuperación de pérdida de datos, planes de contingencia, políticas de respaldo periódico de la información, y otros.

- **Controles para riesgos de confiabilidad:** Cifrado o encriptación, controles de acceso lógico y físicos a los sistemas y servidores, procedimientos de manipulación de copiado, almacenamiento, transmisión y destrucción, documentos reservados con niveles de acceso determinados, protocolos de seguridad sobre Internet (SSL), firewalls, entre otros.

ANEXO Nº 9

CONCEPTOS GENERALES SOBRE REQUISITOS O NORMAS DE CONTROL BÁSICOS CONSIDERADOS EN EL MODELO

1.- Definición de control

El Control es un proceso que permite medir el desempeño individual y organizacional para asegurar que razonablemente las actividades se ajusten a los planes y metas y, mitiguen adecuadamente los riesgos.

El control ha sido definido bajo dos grandes puntos de vista, un punto de vista limitado y un punto de vista amplio. Desde el punto de vista limitado, puede señalarse que, el control se concibe como la verificación a posteriori de los resultados conseguidos en el seguimiento de los objetivos planteados y el control de gastos invertido en el proceso realizado por los niveles directivos.

Desde un punto de vista amplio, puede señalarse que el control es una actividad no sólo a nivel directivo, sino de todos los niveles y miembros de la entidad, orientando a la organización hacia el cumplimiento de los objetivos propuestos bajo mecanismos de medición cualitativos y cuantitativos. Este enfoque hace énfasis en los factores sociales y culturales presentes en el contexto institucional ya que parte del principio que es el propio comportamiento individual quien define en última instancia la eficacia de los métodos de control elegidos por la gestión

El control es una etapa primordial en la administración, pues, aunque una entidad tenga excelentes controles teóricos, una estructura organizacional adecuada y una dirección eficiente, es necesario que exista un mecanismo que verifique e informe si los hechos y actividades de la entidad se están desarrollando según los objetivos.

2. Requisitos de un buen control

Un control, para poder ser declarado como bueno debe tener las siguientes propiedades:

- Corrección de fallas y errores: El control debe detectar e indicar errores de planeación, organización o dirección.
- Previsión de fallas o errores futuros: el control, al detectar e indicar errores actuales, debe prevenir errores futuros, ya sean de planeación, organización o dirección.

3. Importancia del control

El control es importante por que permite medir el desempeño organizacional y cómo se van cumpliendo los objetivos de una entidad. Hasta el mejor de los planes se puede desviar. El control se emplea para:

- Mejorar la calidad: Las fallas del proceso se detectan y el proceso se corrige para eliminar errores.

- Enfrentar el cambio: Este forma parte ineludible del ambiente de cualquier organización. Las directrices de gobierno cambian, el comportamiento de los usuarios de los servicios o beneficios se modifica, surgen exigencias nuevas, aparecen tecnología emergentes, se aprueban o modifican leyes y reglamentos, etc. La función del control sirve a la dirección para responder a las amenazas o las oportunidades de todo ello, porque les ayuda a detectar los cambios que están afectando los productos y los servicios de sus organizaciones.
- Agregar valor: Los tiempos veloces de los ciclos son una manera de obtener ventajas competitivas. El principal objetivo de una organización debería ser "agregar valor" a su producto o servicio, de tal manera que los usuarios puedan aprovechar eficiente y eficazmente sus beneficios. Con frecuencia, este valor agregado adopta la forma de una calidad por encima de la medida lograda aplicando procedimientos de control.
- Facilitar la delegación y el trabajo en equipo: La tendencia contemporánea hacia la administración participativa también aumenta la necesidad de delegar autoridad y de fomentar que los empleados trabajen juntos en equipo. Esto no disminuye la responsabilidad última de la dirección. Por el contrario, cambia la índole del proceso de control. Por tanto, el proceso de control permite que la dirección controle el avance de los funcionarios, sin entorpecer su creatividad o participación en el trabajo.

4.- Secuencia típica de control

- Fijación de estándares: Es la primera etapa del control, que establece los estándares o criterios de evaluación o comparación. Un estándar es una norma o un criterio que sirve de base para la evaluación o comparación de alguna cosa.
- Selección de puntos críticos de control: Debe definirse cuáles serán los puntos o aspectos claves de control que deben monitorearse.
- Comparación y verificación contra los estándares. Se compara el desempeño con lo que fue establecido como estándar, para verificar si hay desvío o variación, esto es, algún error o falla con relación al desempeño esperado.
- Reporte de desviaciones significativas al nivel jerárquico correspondiente. En el caso de existir desviaciones del estándar, debe informarse al jefe correspondiente
- Tomar acciones correctivas. La acción correctiva es siempre una medida de corrección y adecuación de algún desvío o variación con relación al estándar esperado.
- Determinación si la acción tomada es efectiva para corregir las desviaciones tomadas.
- Revisar y modificar los estándares si corresponde.

5.- Requisitos o normas básicas de control consideradas en el modelo

Son los medios, mecanismos o procedimientos que permiten alcanzar los objetivos de control. Comprenden las políticas específicas, los procedimientos, los planes de la organización (incluida la división de las tareas) y los dispositivos físicos (tales como cerraduras o alarmas contra incendio), si bien no se limitan exclusivamente a estos aspectos. Los controles deben proporcionar una seguridad razonable de que se logren continuamente los objetivos del control interno. Para ello, deben ser eficaces y estar diseñados de forma que operen como un sistema integrado y no individualmente.

Los controles, para que sean eficaces, deben cumplir con el propósito previsto en la aplicación real. Es posible que los controles diseñados para funcionar en un ambiente manual no sean eficaces en uno automatizado. Por consiguiente, los controles seleccionados deben cumplir el propósito previsto y funcionar siempre que el caso lo requiera. En cuanto a su eficiencia, los controles deben estar diseñados para poder obtener el máximo beneficio con un esfuerzo adecuado. Los controles que se examinen para verificar su eficacia y suficiencia deben ser los que se utilizan en la práctica y deben ser evaluados periódicamente para asegurar su aplicación constante en la prevención de riesgos.

Los controles que se presentan a continuación son los que se utilizan generalmente en una estructura de control interno ordenada y eficaz. Los métodos y procedimientos específicos que se describen en relación a cada uno de ellos, no pretenden ser exhaustivos sino que deben ser considerados como ejemplos. Entre otros se cuentan: la organización, la documentación, el registro oportuno y adecuado de las transacciones y hechos, autorización y ejecución de las transacciones y hechos, división de las tareas, supervisión y acceso a los recursos y registros y responsabilidad ante los mismos.

a) Documentación en papel y medios electrónicos

Deben documentarse las estructuras de control interno y todas las transacciones y hechos internos, incluyendo sus objetivos y procedimientos de control, y todos los aspectos pertinentes de las transacciones y hechos significativos. Asimismo, la documentación en papel y electrónica debe estar disponible y ser fácilmente accesible para su verificación por el personal apropiado y los auditores.

La documentación relativa a las estructuras de control interno debe incluir aspectos sobre la estructura y políticas de una institución, sobre sus categorías operativas, objetivos y procedimientos de control. Esta información debe figurar en documentos tales como planes o guías, las políticas administrativas y los manuales de operación y de contabilidad.

La documentación sobre transacciones y hechos significativos debe ser completa y exacta y facilitar el seguimiento de la transacción o hecho, antes, durante y después de su realización.

La documentación de las estructuras de control interno, de las transacciones y de hechos importantes debe tener un propósito claro, ser apropiada para alcanzar los objetivos de la institución y servir a los directivos para controlar sus operaciones y a los auditores para analizar dichas operaciones.

En los casos en que existen sistemas informáticos integrados en la institución, que generen como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas, integridad, completitud, archivo o registro, accesibilidad y disponibilidad y no-repudio de la información.

b) Registro oportuno y adecuado de las transacciones y hechos

Las transacciones y hechos importantes deben registrarse inmediatamente y debidamente clasificados.

Las transacciones deben registrarse en el mismo momento en que ocurren a fin de que la información siga siendo relevante y útil para los directivos que controlan las operaciones y adoptan las decisiones pertinentes. Ello es válido para todo el proceso o ciclo de vida de una transacción; abarcando el inicio y la autorización, todos los aspectos de la transacción mientras se realiza y su anotación final en los registros. También conviene actualizar rápidamente toda la documentación con objeto de mantener su validez.

Se requiere, asimismo, una clasificación pertinente de las transacciones y hechos a fin de garantizar que la dirección disponga continuamente de una información fiable. Una clasificación pertinente significa organizar y procesar la información a partir de la cual se elaboran los informes, los planes y los estados financieros y presupuestarios.

El registro inmediato y pertinente de la información es un factor esencial para asegurar la oportunidad y fiabilidad de toda la información que la institución maneja en sus operaciones y en la adopción de decisiones.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto de la firma, integridad, completitud y archivo o registro.

c) Autorización y ejecución de las transacciones y hechos

Las transacciones y hechos relevantes solo podrán ser autorizados en papel o electrónicamente y ejecutados por aquellas personas que actúen dentro del ámbito de sus competencias.

La dirección es quien decide el canje, la transferencia, la utilización o la asignación de fondos para atender metas específicas en condiciones particulares. La autorización es la principal forma de asegurar que sólo se efectúen transacciones y hechos válidos de conformidad con lo previsto por la dirección. La autorización debe estar documentada física o electrónicamente y ser comunicada explícitamente a los directivos y a los empleados, incluyendo los términos y condiciones específicos conforme a los cuales se concede una autorización. La conformidad con los términos de una autorización significa que los empleados ejecutan las tareas que les han sido asignadas de acuerdo con las directrices y dentro del ámbito de competencias establecido por la dirección o la legislación.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas e integridad de la información.

d) División de las tareas

Las tareas y responsabilidades principales ligadas a la autorización, tratamiento, registro y revisión de las transacciones y hechos deben ser asignadas a personas diferentes.

Con el fin de reducir el riesgo de errores, despilfarros o actos ilícitos, o la probabilidad de que no se detecten este tipo de problemas, es preciso evitar que todos los aspectos fundamentales de una transacción u operación se concentren en manos de una sola persona o sección. Las funciones y responsabilidades deben asignarse sistemáticamente a varias personas para asegurar un equilibrio eficaz entre los poderes. Entre las funciones claves figuran la autorización y el registro de las transacciones, la emisión y el recibo de los haberes, los pagos y la revisión o fiscalización de las transacciones. Sin embargo, la colusión puede reducir o eliminar la eficacia de esta técnica de control interno.

Una pequeña organización puede que no tenga suficientes empleados para aplicar esta técnica plenamente. En tal caso, la dirección debe ser consciente del riesgo que ello implica y compensar el defecto con otros controles. La rotación del personal contribuye a que los aspectos centrales de las transacciones o hechos contables no se concentren en una sola persona por un espacio de tiempo prolongado. Debe promoverse e incluso exigirse también el uso del período vacacional anual para ayudar a reducir estos riesgos.

e) Supervisión

Debe existir una supervisión para garantizar el logro de los objetivos de control interno.

Los supervisores deben examinar y aprobar cuando proceda, el trabajo encomendado a sus subordinados. Asimismo, deben proporcionar al personal las directrices y la capacitación necesarias para minimizar los errores, el despilfarro y los actos ilícitos y asegurar la comprensión y cumplimiento de las directrices especificas de la dirección.

La asignación, revisión y aprobación del trabajo del personal exige:

- Indicar claramente las funciones y responsabilidades del trabajo del empleado.
- Examinar sistemáticamente el trabajo de cada empleado, en la medida que sea necesario.
- Aprobar el trabajo en puntos críticos del desarrollo para asegurarse de que avanza según lo previsto.

La asignación, revisión y aprobación del trabajo del personal debe tener como resultado el control apropiado de sus actividades. Ello incluye: la observancia de los procedimientos y requisitos aprobados, la constatación y eliminación de los errores, los malentendidos y las prácticas inadecuadas, la reducción de las probabilidades de que ocurran o se repitan actos ilícitos y el examen de la eficiencia y eficacia de las operaciones. La delegación del trabajo de los supervisores no exime a estos de la obligación de rendir cuentas de sus responsabilidades y tareas.

f) Acceso a los recursos y registros y responsabilidades ante los mismos

El acceso a los recursos y registros debe limitarse a las personas autorizadas para ello, quienes están obligadas a rendir cuentas de la custodia o utilización de los mismos. Para garantizar dicha responsabilidad, se debe cotejar periódicamente los recursos con los registros y verificar si coinciden. La frecuencia de estas comparaciones depende de la vulnerabilidad y relevancia de los activos.

La restricción del acceso físico y lógico a los recursos permite reducir el riesgo de una utilización no autorizada o de pérdida y contribuir al cumplimiento de las directrices de la dirección. El grado de limitación depende de la vulnerabilidad de los recursos y del riesgo potencial de pérdida. Ambos deben evaluarse periódicamente. Por ejemplo, el acceso a los documentos sumamente vulnerables y la responsabilidad ante los mismos, tales como cheques en blanco, puede restringirse:

- Manteniéndolos en una caja fuerte.
- Asignando a cada documento un número de serie.
- Encargando su custodia a personas responsables.
- Al determinarse la vulnerabilidad de un activo, debe considerarse también su costo, la facilidad de transporte y el riesgo de pérdida o de utilización indebida.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas, integridad y accesibilidad y disponibilidad. Además de deberá evaluar los niveles de seguridad de los accesos lógicos a las base de datos de la organización.

6.- Estructura general del Marco Integrado de control Interno – Modelo C.O.S.O.

El ambiente de control da el tono de una organización, influenciando la conciencia de control de sus empleados; es el fundamento de todos los demás componentes del control interno, proporcionando disciplina y estructura. Es necesario comprender, evaluar y obtener evidencia sobre la efectividad de cualquier control en el cual se desea confiar para determinar la naturaleza, alcance y oportunidad del trabajo de auditoría que debe efectuarse.

La estructura genérica que se presenta es sólo a modo explicativo, puesto que su existencia y características dependen del tipo de control y de la estructura del proceso, entre otras variables. El lector puede encontrar suficiente literatura del Modelo C.O.S.O., incluida la Internet.

- Normas relativas al ambiente de control
    - Ambiente propicio para el control.
    - Actitud de apoyo superior al control interno.
    - Valores de integridad y ética.
    - Administración eficaz del potencial humano.

- Estructura organizativa formal y conocida.
- Delegación formal y adecuada.
- Coordinación de acciones organizacionales.
- Participación del personal en el control interno.
- Adhesión a las políticas institucionales.

❑ Normas relativas a la evaluación de riesgos

- Identificación y evaluación de riesgos.
- Planificación formal.
- Indicadores de desempeño mensurables.
- Divulgación de los planes.
- Definición y comunicación de políticas de apoyo a los objetivos.
- Revisión de los objetivos.
- Cuestionamiento periódico de los supuestos de planificación.

❑ Normas relativas a las actividades de control

- Prácticas y medidas de control formales.
- Control integrado.
- Análisis de costo/beneficio.
- Responsabilidad delimitada.
- Instrucciones por escrito.
- Separación de funciones incompatibles.
- Autorización y aprobación de transacciones y operaciones.
- Documentación de procesos y transacciones.
- Supervisión constante.
- Registro oportuno.
- Sistema contable y presupuestario.
- Acceso a activos y registros.
- Revisiones de control permanentes.
- Conciliación periódica de registros.
- Inventarios periódicos.
- Arqueos independientes.
- Formularios uniformes.
- Rotación de labores.
- Toma oportuna de vacaciones.
- Garantías a favor de la institución.
- Dispositivos de control y seguridad lógicos y físicos.

❑ Normas relativas a información y comunicación

- Obtención y comunicación de información efectivas.
- Calidad y suficiencia de la información.
- Sistemas de información.
- Controles sobre sistemas de información.
- Canales de comunicación abiertos.
- Archivo institucional formal.

- Normas relativas al monitoreo

  - Monitoreo constante del control interno en operación.
  - Monitoreo de las actividades.
  - Monitoreo constante del ambiente de control.
  - Evaluación del desempeño institucional.
  - Informes de seguimiento a responsables.
  - Rendición de cuentas.
  - Reporte de deficiencias.
  - Toma de acciones correctivas.
  - Asesoría externa para monitoreo del control interno.

7.- Identificación y análisis de controles claves

Identificados los riesgos, es necesario identificar y analizar los controles claves existentes en la institución, los que teóricamente mitigan los riesgos, esto es, todas las medidas que ha tomado la administración con la finalidad de evitar la ocurrencia de un riesgo potencial. Estos controles deben ser evaluados en el nivel de cumplimiento de normas de control y calificados de acuerdo a su diseño, es decir, su oportunidad (en que momento del proceso se aplican; preventivos, correctivos, detectivos), periodicidad (si son permanentes, periódicos u ocasionales), grado de automatización (manual, semi automatizado, 100% automatizado) y evaluados en términos del cumplimiento de normas específicas de control.

Una vez determinada claramente la existencia de todos los controles asociados a los riesgos relevantes que operan en el proceso en estudio, será necesario en primer lugar, definir si existe uno o más controles asociados a cada riesgo específico identificado.

Cuando exista más de un control por riesgo específico, será necesario identificar si se trata de controles cuya presencia es clave o fundamental para mitigar la ocurrencia del riesgo, o si alguno de los controles no tienen esa característica y sólo se trata de controles que no contribuyen significativamente a mitigar el riesgo. En general para este último tipo de controles, es recomendable informar a la Dirección, para su eliminación o fortalecimiento, si corresponde (relación costo/beneficio).

Cuando se identifique que un riesgo específico tiene varios controles asociados y éstos tienen distinto nivel de efectividad medida en forma individual, el auditor debe sólo evaluar el nivel de efectividad que se genera al actuar en conjunto los distintos controles clasificados como claves, desechando para efectos de este análisis a los controles no fundamentales (ver ejemplo en páginas siguientes).

El segundo paso corresponde a determinar (identificar, analizar y cuantificar) el nivel de efectividad de los controles en base al diseño del control y cumplimiento de normas específicas de control. Nivel definida por los atributos periodicidad, oportunidad y nivel de automatización del control en base al esquema que se presenta en la página siguiente.

El siguiente paso corresponde a analizar para cada uno de los controles claves identificados con los riesgos, el grado de cumplimiento de normas específicas de control.

En resumen, lo que se persigue con este procedimiento, no es sólo verificar la existencia y el grado de cumplimiento de normas específicas para todos los controles, sino que

evaluar si existen controles claves o fundamentales asociados a un riesgo en particular y si éstos además de cumplir con normas específicas están diseñados con la finalidad de mitigar los efectos que se puedan producir ante la materialización del riesgo.

A continuación se presenta un procedimiento que permite dejar evidencia del análisis realizado al auditor. Para este efecto, se sugiere utilizar el siguiente esquema:

Esquema N° 12. Análisis de controles claves

Etapa	Riesgo Relevante	Descripción del Control identificado en el proceso (asociado a un riesgo determinado)	Importancia del control presente para mitigar los riesgos al interior del proceso	
			Clave/Fundamental	No es fundamental

Ejemplo de determinación de una evaluación de la efectividad de los controles claves:

i.- **Esquema N° 13. Ejemplo para identificación de controles claves en la etapa "cálculo de horas extraordinarias"**

Etapa	Riesgo Relevante	Descripción del Control identificado en el proceso (asociado a un riesgo determinado)	Importancia del control presente para mitigar los riesgos al interior del proceso	
			Clave/ fundamental	No es fundamental
Cálculo de horas extraordinarias	Errores o irregularidades en el cálculo de las horas extraordinarias	El sistema de control biométrico registra las horas trabajadas y calcula aquellas que exceden de las 44 horas ordinarias	**X**	
		El jefe de la Unidad de remuneraciones revisa y aprueba el cálculo de horas para su pago.	**X**	
		El encargado de remuneraciones lleva un archivador con el detalle del las horas extras por funcionario		**X**

En este caso, se identifican tres controles mitigantes asociados directamente o indirectamente al riesgo "Errores o irregularidades en el cálculo de las horas extraordinarias", por lo que debe realizarse en primer lugar un análisis de la importancia de cada control para mitigar el riesgo, es decir, determinar si se trata de un control clave.

El resultado del análisis muestra en el ejemplo que, el control descrito como "El encargado de remuneraciones lleva un archivador con el detalle del las horas extras por funcionario", no es un control clave, por lo que no se analizará en cuanto al nivel de cumplimiento con los requisitos o normas que considera el modelo.

ii.- Esquema N° 14. Ejemplo: Análisis del cumplimiento de requisitos del modelo de control en el control mitigante examinado

Riesgo Relevante	Nivel de cumplimento de normas del control asociado Niveles de cumplimiento de normas: adecuado, regular, insuficiente					
	Documentación	Registro	Autorización	División o Segregación	Supervisión	Acceso
Errores o irregularidades en el cálculo de las horas extraordinarias	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel regular
Conclusión del nivel de cumplimiento de las normas: **Adecuado**						

iii.- Esquema N° 11. Ejemplo: Determinación de la efectividad de los controles claves

Controles Claves/fundamental	Nivel de Cumplimiento de normas específicas de control	Características en el diseño del control clave/fundamental				
		Oportunidad	Periodicidad	Automatización	Clasificación	Valor
El sistema biométrico de control horario, contiene un algoritmo que calcula las horas trabajadas, indicando en forma precisa aquellas que exceden de las 44 semanales. El jefe de remuneraciones revisa el reporte del sistema y aprueba el cálculo para su pago.	Adecuado respecto a los requisitos de control del modelo	Preventivo (previene errores y se encuentra al principio del proceso)	Periódico (a la fecha de corte mensual para pago)	Automatizado y Manual	Óptimo	5

8.- Limitaciones de un sistema de control interno

Ningún sistema de control interno puede garantizar su cumplimiento de sus objetivos ampliamente, de acuerdo a esto, el control interno brinda una seguridad razonable en función de:

- Costo beneficio: El control no puede superar el valor de lo que se quiere controlar.
- La mayoría de los controles hacia transacciones o tareas ordinarias: Debe establecerse el control bajo las operaciones repetitivas y en cuanto a las extraordinarias, existe la posibilidad que el sistema no sepa responder.
- El factor de error humano.
- Posibilidad de colusiones que puedan evadir los controles. Colusión y fraude por acuerdo entre dos o más personas para infringir un control. No hay sistema de control invulnerable a estas circunstancias.

ANEXO Nº 10

EJEMPLO INFORMACIÓN PARA EL TRATAMIENTO DE RIESGOS

Proceso transversal (1)	Proceso (2)	Ranking de procesos (3)	Subproceso (4)	Etapa (5)	Riesgo Específico (6)	Fuente del riesgo (7)	Tipo de riesgo (8)	Estrategia genérica (9)	Descripción de la estrategia a aplicar (10)	Efecto potencial en la severidad de riesgo y/o efectividad del control (11)	Responsable de la estrategia (12)	Plazo (13)	Indicador de logro (14)	Periodo Medición del indicador (15)	Meta (16)	Evidencia que se observará (17)
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Falta de garantías	Interna	Procesos	Reducir	Se establecerá una instancia de revisión del Comité de Crédito que deberá revisar cada crédito y cotejar la garantía de acuerdo al tipo de crédito Se adicionará un módulo al sistema de información de créditos, para que si un crédito no tiene incorporado el número de póliza de garantía no permita cursar el crédito	Las acciones tienden a mejorar el control del riesgo que es débil estableciendo una instancia que controle al Comité de Crédito y una aplicación al sistema. También se espera disminuir la probabilidad que se concrete la falta de garantías	Jefe de Operaciones	6 meses	Porcentaje créditos sin garantía (Nº total de créditos mensuales / Nº de créditos sin garantía) * 100	mensual	- 3%	Carpeta del crédito Información del sistema Actas Comité Actas de revisión

ANEXO 11 - 1/2

MATRIZ DE RIESGOS ESTRATÉGICA – OBJETIVO GUBERNAMENTAL DE AUDITORÍA - Nº 3

Levantamiento de información de procesos							Riesgos Identificados								
Proceso Transversal	Proceso	Pd. (1)	Subproceso	Pd. (2)	Etapas	Objetivos	Descripción Riesgos específicos	Fuente de Riesgos	Tipo de riesgo	Probabilidad		Impacto		Severidad del riesgo	
										Clasif.	valor	Clasif	valor	Clasif	valor
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Postulación	10%	…	….	…	…	…	…	…	…	…	…	…
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Evaluación	35%	….	….	…	…	…	…	…	…	…	…	…
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Entrega de créditos	20%	…	…	..	…	…	…	…	…	…	…	…
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Cobranza	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Falta de acciones oportunas de cobranza	Interna	Procesos	Moderado	3	Moderado	3	Alto	9
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Cobranza	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Insolvencia de los deudores	Externa	Económico	Improbable	2	Mayores	4	Alto	8
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Cobranza	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Falta de garantías	Interna	Procesos	Muy improb.	1	Mayores	4	Alto	4
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Ingreso fondos	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Ingreso inoportuno o incompleto de pagos	Interna	Personas	Probable	4	Moderado	3	Alto	12
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Ingreso fondos	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Errores en la digitación de los montos	Interna	Personas	Moderado	3	Mayores	4	Extremo	12
Crédito – Recuperación de prestamos	Créditos de fomento a mujeres microempresarias	35%	Recuperación del crédito	35%	Ingreso fondos	Obtener el pago completo y oportuno de los créditos otorgados a las usuarias	Problemas en la transformación de la información del sistema del Servicio al SIGFE	Interna	Tecnológico	Improbable	2	Mayores	4	Alto	8
Recursos Humanos	…	10%	…	…	…	…	…	…	…	…	…	…	…	…	…
Capacitación	…	25%	…	…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Continúa en la página siguiente

(1) Ponderación estratégica del proceso en relación a los objetivos estratégicos y la misión.
(2) Ponderación estratégica del subproceso en relación a los objetivos del proceso.

ANEXO 11 - 2/2

MATRIZ DE RIESGOS ESTRATÉGICA – OBJETIVO GUBERNAMENTAL DE AUDITORÍA - Nº 3

Viene de la página anterior

Controles claves existentes						Valor y clasificación de la exposición al riesgo ponderada											
						Riesgo		Etapa		Subproceso				Proceso			
Descripción control	Cumple norma de control	Nivel de eficiencia			valor	Nivel ER (3)	Valor ER (3)	Nivel ER (3)	Valor ER (3)	Nivel ER (3)	Valor ER (3)	Valor ERP (4)	Ranking	Nivel ER (3)	Valor ER (3)	Valor ERP (4)	Ranking
		PD	O	A													
…	…	…	…	…	…	Mayor	6	Mayor	6	Mayor	6	0,6	3º	Media	3,8	1,33	1º
…	…	…	…	…	…	Media	3	Media	3	Media	3	1,05	2º	Media	3,8	1,33	1º
…	…	…	…	…	…	menor	2,5	menor	2,5	menor	2,5	0,5	4º	Media	3,8	1,33	1º
El Sistema avisa los vencimiento al Jefe de Cobranzas El Jefe finanzas revisa mensualmente las cobranzas	Si	Pd	Cr	Si	3	Media	3	Mayor	5	medio	3,8	1,33	1º	Media	3,8	1,33	1º
Sin control	-	-	-	-	1	No aceptable	8	Mayor	5	medio	3,8	1,33	1º	Media	3,8	1,33	1º
El Comité de crédito no puede entregar crédito sin garantía	No	-	-	-	1	Mayor	4	Mayor	5	medio	3,8	1,33	1º	Media	3,8	1,33	1º
El Tesorero ingresa los pagos al sistema que autovalida los datos. Para abonos o pagos fuera de plazo se requiere autorización del superior. Mensualmente los reportes los revisa el jefe de Finanzas	Si	Pe	Pr	Si	5	Menor	2,4	Menor	2,5	medio	3,8	1,33	1º	Media	3,8	1,33	1º
El Tesorero ingresa los pagos al sistema que autovalida los datos. Para abonos o pagos fuera de plazo se requiere autorización del superior. Mensualmente los reportes los revisa el jefe de Finanza	Si	Pe	Pr	Si	5	Menor	2,4	Menor	2,5	medio	3,8	1,33	1º	Media	3,8	1,33	1º
El Jefe de Finanzas revisa la transformación antes de remitirse los datos al exterior	Si	Pd	Cr	M	3	Menor	2,7	Menor	2,5	medio	3,8	1,33	1º	Media	3,8	1,33	1º
…		…	…	…	…	…	…	…	…	…	…	…	….	Mayor	5	0,5	3°
…		…	…	…	…	…	…	…	…	…	…	…	….	Medio	3,9	0,98	2°
…		…	…	…	…	…	…	…	…	…	…	…	….	….	….	….	….

(3) ER= Exposición al Riesgo.
(4) ERP= Exposición al Riesgo Ponderado.