2024

TEC | Tecnológico de Costa Rica

SISTEMA DE CONTROL INTERNO

Guía metodológica para la Autoevaluación del Sistema de Control Interno y la Gestión del Riesgo en el ITCR

Unidad Especializada de Control Interno

ueci@itcr.ac.cr

Guía metodológica para la Autoevaluación del Sistema de Control Interno y la Gestión del Riesgo en el ITCR

Introducción

Con la entrada en vigencia de la Ley General de Control Interno No. 8292, se establece la obligatoriedad para la Contraloría General de la República y todos los entes u órganos sujetos a su fiscalización, de contar con un sistema de control interno que proporcione seguridad en el cumplimiento de sus atribuciones y competencias, a través del aseguramiento de los criterios mínimos para el establecimiento, funcionamiento, mantenimiento, perfeccionamiento y seguimiento de dicho sistema.

Es por ello por lo que, la Oficina de Planificación Institucional mediante la Unidad Especializada de Control Interno, elabora la presente guía metodológica con el fin de orientar la realización de los procesos de autoevaluación y gestión de riesgos, normados en el Reglamento del Sistema de Control Interno en el ITCR.

Cada uno de estos procesos implica la realización de una serie de actividades virtuales o presenciales, mediante la aplicación de instrumentos a través de talleres, entrevistas y acompañamiento técnico con el interesado de la valoración.

Marco Legal

La base normativa en temas referentes a la presente metodología es:

1. Constitución Política de la República de Costa Rica
2. Ley General de Control Interno N°8292
3. Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública.
4. Ley General de la Administración Pública
5. Ley de Administración Financiera
6. Normas de Control Interno para el Sector Público
7. Normas Técnicas para la Gestión y el Control de las Tecnologías de Información
8. Directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgo Institucional
9. Reglamento de Control Interno

La veracidad y exactitud de la información suministrada a la UECI es total responsabilidad de la autoridad que la brinda, según lo establecido en los Artículos Nos. 10, 12 y 16 de la Ley General de Control Interno No. 8292.

Sistema de Control Interno[1]

Se entenderá por Sistema de Control Interno la serie de acciones ejecutadas por la administración activa diseñadas para proporcionar seguridad razonable en la consecución de los siguientes objetivos:

- Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
- Confiabilidad y oportunidad de la información.
- Eficiencia y eficacia de las operaciones.
- Cumplir con el ordenamiento jurídico y técnico.

La responsabilidad del jerarca y del titular subordinado es establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.

Según la Ley General de Control Interno N°8292, los componentes del Sistema de Control Interno se dividen en dos grandes aristas:

Componentes orgánicos

Los componentes orgánicos son las instancias organizacionales que participan en el control interno, identificamos dos: la administración activa y la auditoría interna. Los diferentes alcances y la participación de ellos en el sistema también son considerados en la normativa jurídica y técnica.

Componentes funcionales

Los componentes funcionales, por su parte, deben ser establecidos, mantenidos, perfeccionados y evaluados de acuerdo con las responsabilidades que competen a las diferentes instancias institucionales.

[1] Ley General de Control Interno N°8292
Normas de Control Interno para el sector público (N-2-2009-CO-DFOE)

- **Ambiente de Control**

Es el conjunto de factores del ambiente organizacional que las autoridades y demás funcionarios deben establecer y mantener, para permitir el desarrollo de una actitud positiva y de apoyo para el control interno.

- **Valoración del Riesgo**

Consiste en la identificación y el análisis de los riesgos que enfrenta la institución, provenientes tanto de fuentes internas como externas, que son relevantes para la consecución de los objetivos, a partir de lo cual el jerarca y los titulares subordinados deben realizar los esfuerzos pertinentes con el fin de determinar cómo se deben administrar dichos riesgos.

- **Actividades de Control**

Se refiere a los métodos, políticas, procedimientos y otras medidas establecidas y ejecutadas como parte de las operaciones para asegurar que se están aplicando las acciones necesarias para manejar y minimizar los riesgos y realizar una gestión eficiente y eficaz.

- **Sistema de Información**

Referido a los sistemas de información y comunicación existentes en el ITCR, los cuales deben permitir la generación, la captura, el procesamiento y la transmisión de información relevante sobre las actividades del Instituto y los eventos internos y externos que puedan afectar su desempeño positiva o negativamente.

- **Seguimiento**

Comprende todas las actividades que se llevan a cabo para valorar la calidad del funcionamiento de la gestión institucional y del sistema de Control Interno.

Vinculación del Sistema de Control Interno con la calidad

El jerarca y los titulares subordinados, según sus competencias, deben promover un compromiso institucional con la calidad y apoyarse en el Sistema de Control Interno para propiciar la materialización de ese compromiso en todas las actividades y actuaciones de la organización. A los efectos, deben establecer las políticas y las actividades de control pertinentes para gestionar y verificar la calidad de la gestión, para asegurar su conformidad con las necesidades institucionales, a la luz de los objetivos, y con base en un enfoque de mejoramiento continuo (1.9 Normas de Control Interno para el Sector Público).

Autoevaluación del Sistema de Control Interno

La Autoevaluación es un diagnostico que permite el fortalecimiento organizacional con la revisión y análisis de las fortalezas y debilidades de sus actividades a la luz de los componentes del Sistema de control interno, identificando las mejoras posibles para el corto, mediano y largo plazo.

El jerarca y los titulares subordinados, según sus competencias, deben disponer la realización, por lo menos una vez al año, de una autoevaluación del SCI, que permita identificar oportunidades de mejora del sistema, así como detectar cualquier desvío que aleje a la institución del cumplimiento de sus objetivos. (6.3.2 Normas de Control Interno para el Sector Público)

Objetivos

a. Analizar y revisar las actividades que desarrolla una dependencia a la luz de los componentes del sistema de control interno, para identificar fortalezas y/o debilidades que se requieren actualizar, modificar o eliminar.

b. Determinar e incorporar dentro del plan de mejoras aquellas actividades a realizar en el corto y mediano plazo que permitan subsanar las debilidades del sistema de control interno.

c. Documentar, comunicar y dar seguimiento a la realización del proceso de autoevaluación para cumplir con las disposiciones jurídicas.

Etapas y responsables

Según la etapa en la cual se desarrolla el proceso de Autoevaluación del Sistema de Control Interno, los responsables son:

Etapa	***Actividad***	***Responsable***
I. Diseño de la Autoevaluación	-Preparación de cronograma -Preparación de la propuesta del instrumento para la autoevaluación -Revisión de la propuesta la autoevaluación (Coordinación y Dirección) -Envío de correo/oficio para informar sobre el inicio del proceso -Revisión del sistema automatizado (actualizar y habilitar usuarios) -Apertura del proceso	UECI
II. Desarrollo de la Autoevaluación	-Inducción a usuarios nuevos -Ingreso al sistema para realizar autoevaluación -Comprobar que los usuarios estén ejecutando el proceso de autoevaluación.	UECI Personas responsables de ejecutar el proceso
III. Resultados	-Revisión de los cuestionarios completados	UECI

Etapa	*Actividad*	*Responsable*
IV. Seguimiento	-Preparación de insumos para el informe -Elaboración del Informe -Presentación del Informe ante las autoridades -Definir cronograma de seguimiento -Elaborar correo/oficio para dar por iniciado el proceso de seguimiento - Revisión del sistema automatizado (actualizar y habilitar usuarios) -Apertura del sistema -Aplicación del seguimiento -Revisión de los cuestionarios completados -Preparación de insumos para el informe -Elaboración del Informe -Presentación del Informe ante las autoridades	UECI Personas responsables de ejecutar el proceso

Considerando que la Auditoría Interna aplica sus propias autoevaluaciones se excluyen de realizar el proceso de Autoevaluación Institucional.

Alcance

La Autoevaluación del Sistema de Control Interno será aplicada a las actividades y procesos de las dependencias del ITCR, así como a temas específicos tales como las Tecnologías de Información u otro que se considere necesario.

Producto

- Identificación de las debilidades y fortalezas del sistema de control interno según los componentes funcionales.
- Definición de acciones de mejora, responsables y plazos de ejecución.
- Grado de avance de las mejoras efectuadas y su impacto a nivel institucional.
- Seguimiento al Plan de acción de mejora.

Comunicación y documentación

Los productos de la Autoevaluación del Sistema de Control Interno son presentados por la Unidad Especializada de Control Interno ante el Consejo de Rectoría y enviados al Consejo Institucional y la Auditoría Interna para su conocimiento.

Instrumento

El cuestionario deberá actualizarse previo a cada proceso, el mismo debe incluir los componentes funcionales del Sistema de Control Interno.

La estructura de los criterios para responder será:

Escala de Criterios de Autoevaluación

ITEM	*DESCRIPCIÓN*	*DOCUMENTO DE REFERENCIA*
SI	La respuesta "SI" debe utilizarse cuando se cumpla más del 75% de lo preguntado.	*
NO	La respuesta "NO" debe utilizarse cuando se cumpla un 25% o menos de los preguntado	**
PARCIAL	La respuesta "PARCIALMENTE" se debe utilizar cuando lo preguntado se cumpla en un rango superior al 25%, pero menor al 75%.	**
N/A	La respuesta "N/A" se debe utilizar si de las anteriores opciones ninguna aplica.	

* En el caso de las respuestas positivas, se solicita indicar la referencia del documento probatorio.

** Las respuestas dadas en negativo y de manera parcial permiten evidenciar las debilidades que actualmente se presentan en la dependencia y que impiden ejecutar las actividades de una manera más efectiva, generando un plan de mejora, el cual se debe incorporar como actividad del Plan Anual Operativo y Plan de Trabajo según corresponda.

Seguimiento

Se procederá a dar seguimiento a las acciones de mejora producto de la autoevaluación del Sistema de Control Interno una vez al año, presentando a la administración y a los responsables de la ejecución del proceso el informe final de autoevaluación, el cual se estructura con el resultado de los análisis y juicios emitidos sobre la calidad de cada uno de los componentes del sistema de control; las fallas de control detectadas, y las acciones de mejora a realizar para lograr una efectividad mayor de dicho sistema y así permitir a la institución cumplir con sus objetivos.

Gestión de Riesgo

La gestión del riesgo debe ser una parte de, y no estar separada de la misión, la visión, el liderazgo y compromiso, la estrategia, los objetivos y la operación de la institución.

Objetivo

Aplicar el proceso de gestión de riesgo y dar seguimiento al plan de acción de respuesta al riesgo producto de la valoración realizada a los planes de corto, mediano y largo plazo u otra valoración solicitada, para mitigar y controlar los riesgos, mediante herramientas tecnológicas y metodologías que permitan facilitar la ejecución del proceso.

Conceptos

Riesgo: Probabilidad de que ocurran eventos que tendrían consecuencias sobre el cumplimiento de los objetivos planteados fijados.

Riesgo de largo plazo (estratégico): aquel que afecta o amenace el cumplimiento de la misión, visión, valores, objetivos estratégicos y metas institucionales u otro que se desprende de la estrategia.

Riesgo de mediano plazo: riesgos que afectan la ejecución de los planes tácticos o de inversión

Riesgo de corto plazo: aquellos que afectan la ejecución de los planes anuales operativo y los planes anuales de trabajo.

Alcance

Aplica a personas responsables de la Rectoría, Vicerrectorías, Direcciones de Campus Tecnológicos Locales, Centros Académicos, Dependencias, y Subdependencias que lo soliciten.

Lineamientos de la gestión del riesgo

1. La gestión del riesgo se realizará en los niveles de planificación estratégico, táctico y operativo.

2. La Institución establecerá acciones de respuesta al riesgo para enfrentar las emergencias y desastres, activando los protocolos correspondientes con la finalidad de preservar la salud y mantener la calidad de vida de las personas que integran la Comunidad Institucional.

3. Serán evaluadas las actividades que puedan presentar una interrupción en el quehacer a raíz de la materialización de un riesgo, con el fin de tomar decisiones respecto a la continuidad operativa institucional.

4. Gestionar los riesgos desde la formulación hasta el seguimiento de las acciones de respuesta a los que se expone la Institución, con el fin de

aumentar el nivel de resiliencia como herramienta para la continuidad del negocio.

Responsables

Los responsables de la aplicación, cumplimiento y seguimiento de la gestión del riesgo serán:

Nivel Estratégico: Consejo de Rectoría, quien fungirá como la Comisión Estratégica que apoyará y ejecutará el proceso de valoración de riesgos de las metas institucionales, cumplirá y dará el seguimiento correspondiente al plan de acción de respuesta al riesgo.

Nivel Táctico o de Inversión: Personas responsable de la Rectoría, Vicerrectoría, Directores de Campus Tecnológicos Locales, Centros Académicos, dependencias u oficinas técnicas, según corresponda.

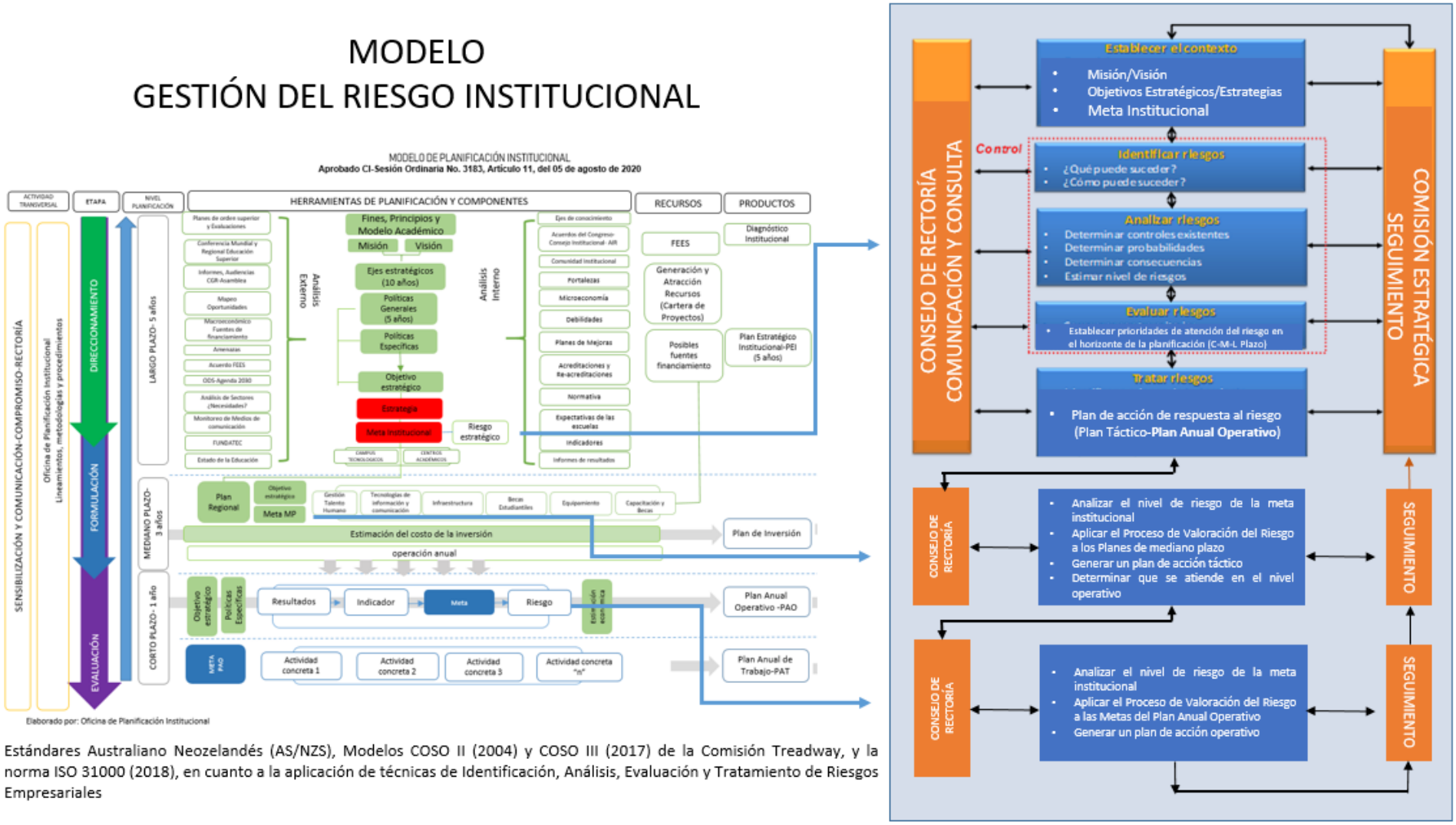
Nivel Operativo: Personas responsable de la Rectoría, Vicerrectoría, Directores de Campus Tecnológicos Locales, Centros Académicos (Plan Anual Operativo), Directores de Escuelas y departamentos (Plan Anual de Trabajo). Y la dependencia que lo solicite mediante un mecanismo formal a la Oficina de Planificación Institucional (objetivos, programas, proyectos, procesos, actividades u otros).

El jerarca, los titulares subordinados y demás personas funcionarias públicas que debiliten con sus acciones el Sistema Específico de Valoración de Riesgos Institucionales u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, estarán sujetos al régimen sancionatorio establecido en el Artículo 39 de la Ley General de Control Interno N°8292.

Modelo de Gestión de Riesgos

A partir del Modelo de Planificación Institucional conocido por el Consejo Institucional en la Sesión Ordinaria No. 3183, Artículo 11 del 5 de agosto del 2020, se diseña el siguiente modelo y procedimiento para la gestión de riesgos institucionales considerando la línea estratégica, táctica y operativa del modelo aprobado.

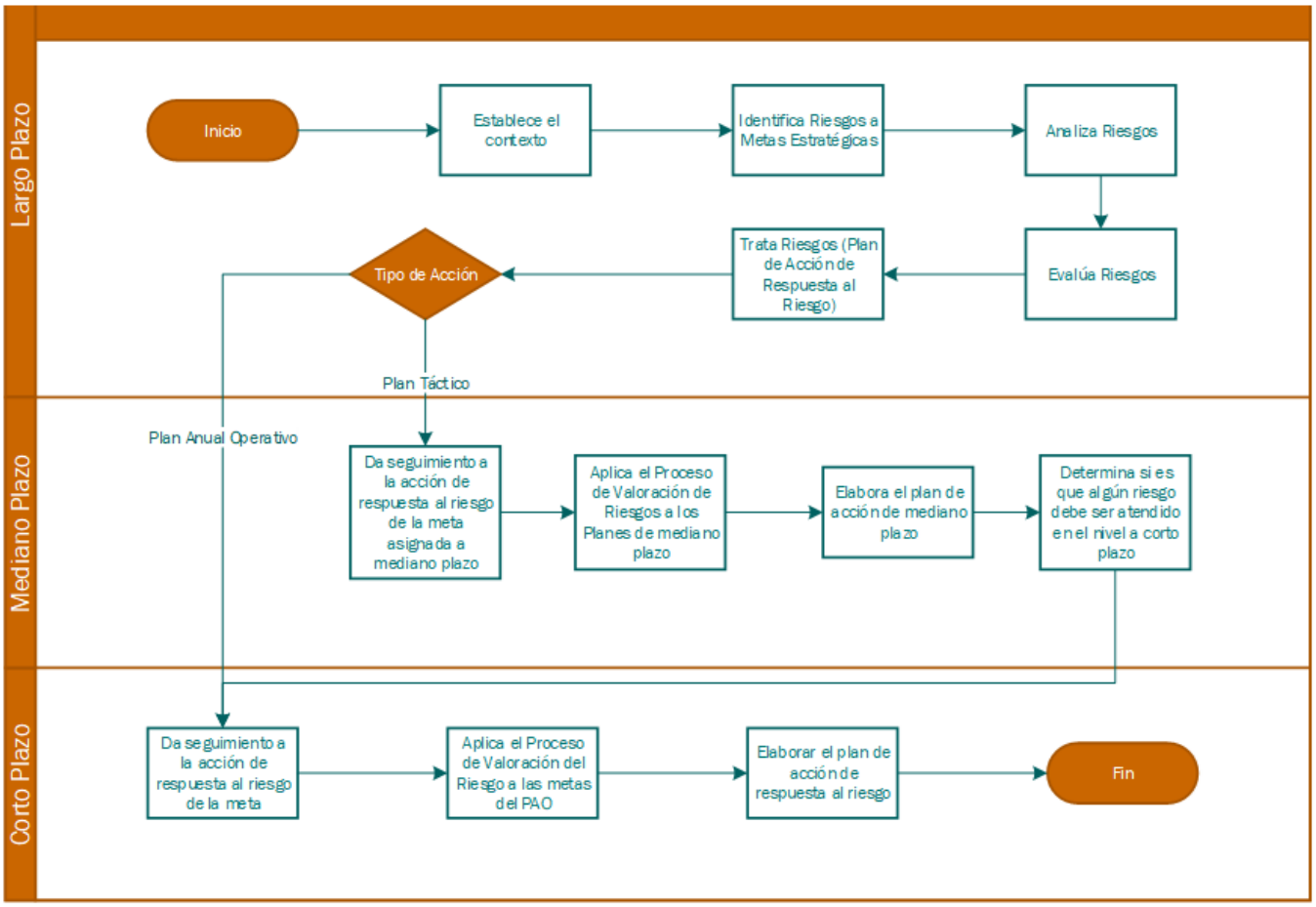
Figura 1. Modelo de Planificación Institucional y Modelo de Gestión de Riesgos



Estándares Australiano Neozelandés (AS/NZS), Modelos COSO II (2004) y COSO III (2017) de la Comisión Treadway, y la norma ISO 31000 (2018), en cuanto a la aplicación de técnicas de Identificación, Análisis, Evaluación y Tratamiento de Riesgos Empresariales

Fuente: Oficina de Planificación Institucional. Unidad Especializada de Control Interno

Procedimiento Gestión del Riesgo



Proceso de Gestión de Riesgos

A continuación, se detalla el proceso de la gestión de riesgos que se ejecuta a nivel institucional:

1. Establecer el contexto: análisis de la misión, visión, objetivos estratégicos, estrategias y metas institucionales.

2. Identificación de riesgos: a partir de las metas institucionales se determina ¿Qué podría suceder? y ¿Cómo podría suceder?

3. Analizar los riesgos: se determina la probabilidad e impacto, considerando la siguiente información:

DESCRIPCION	PROBABILIDAD	DEFINICIÓN
Improbable	0.2	El evento solo podría ocurrir excepcionalmente (con una periodicidad superior a un año)
Poco probable	0.4	El evento podría ocurrir en algún momento (una vez al año)
Probable	0.6	El evento podría ocurrir con cierta periodicidad (una vez por semestre)
Bastante probable	0.8	El evento podría ocurrir en forma recurrente (más de una vez por semestre)
Muy probable	1.0	El evento podría ocurrir en la mayoría de las circunstancias (al menos una vez por mes)

FACTOR	DETALLE
1. Indicadores	Eventos que provoquen una disminución en el porcentaje de cumplimiento del indicador correspondiente a la meta.
2. Ejecución Presupuestaria	Evento que produzca una disminución en la ejecución del presupuesto de egresos asignado por meta en el PAO Presupuesto.

El detalle de la descripción, niveles de impacto y definiciones por factor antes mencionados.

DESCRIPCION	NIVEL DE IMPACTO	DEFINICIÓN
Muy bajo	1	**1. Indicadores:** El impacto será muy bajo cuando se produzca una disminución del porcentaje de cumplimiento del indicador, menor o igual al 5% de lo establecido como indicador para dicha meta en el PAO. **2. Ejecución Presupuestaria:** El impacto será muy bajo cuando se produzca una disminución menor o igual al 10% del monto presupuestado de egresos asignado a la meta.
Bajo	2	**1. Indicadores:** El impacto será bajo cuando se produzca una disminución del porcentaje de cumplimiento del indicador, mayor a 5% y menor o igual a 10% de lo establecido como indicador para dicha meta en el PAO. **2. Ejecución Presupuestaria:** El impacto será bajo cuando se produzca una disminución mayor a 10% o menor o igual al 15% del monto presupuestado de egresos asignado a la meta.
Moderado	3	**1. Indicadores:** El impacto será moderado cuando se produzca una disminución del porcentaje de cumplimiento del indicador, mayor a 10% y menor o igual a 15% de lo establecido como indicador para dicha meta en el PAO. **2. Ejecución Presupuestaria:** El impacto será moderado cuando se produzca una disminución mayor a 15% o menor o igual al 20% del monto presupuestado de egresos asignado a la meta.

DESCRIPCION	NIVEL DE IMPACTO	DEFINICIÓN
Alto	4	1. **Indicadores:** El impacto será alto cuando se produzca una disminución del porcentaje de cumplimiento del indicador, mayor a 15% y menor o igual a 20% de lo establecido como indicador para dicha meta en el PAO. 2. **Ejecución Presupuestaria:** El impacto será alto cuando se produzca una disminución mayor a 20% o menor o igual al 25% del monto presupuestado de egresos asignado a la meta.
Muy alto	5	1. **Indicadores:** El impacto será muy alto cuando se produzca una disminución del porcentaje de cumplimiento del indicador, mayor al 20 % de lo establecido como indicador para dicha meta en el PAO. 2. **Ejecución Presupuestaria**: El impacto será muy alto cuando se produzca una disminución mayor a 25% del monto presupuestado de egresos asignado a la meta.

Seguidamente se evalúa el tipo de control, la madurez y las posibles fallas para determinar la efectividad de estos, obteniendo así el riesgo residual, o bien, el criterio de aceptación.

a. Tipo de Control: Son los mecanismos existentes para mitigar el riesgo.

TIPO DE CONTROL	DEFINICIÓN
Inexistente	No se aplica ningún tipo de control.
Detectivo	Diseñados para identificar y descubrir eventos no deseados después de que ya han ocurrido, pero que por sí mismos no los corrige.
Correctivo	Diseñados para corregir los eventos no deseados detectados. Eliminarán ciertas conductas y resultados indeseables.
Preventivo	Diseñados para evitar los eventos no deseados. Impide que una amenaza llegue siquiera a materializarse.

b. Madurez de Control: La madurez es el punto culminante de un proceso que determina el crecimiento y desarrollo, que consiste en la integración diversos controles.

MADUREZ	DESCRIPCIÓN
Nulo	No existe madurez.
Informal	El control ha sido diseñado e implantado, su aplicación depende de la persona que esté en el puesto. No existe documento formal de aprobación de dicho control ni supervisión de este.
Estandarizado	El control ha sido diseñado, implantado, divulgado, documentado y aprobado, no se ejerce supervisión sobre dicho control.
Monitoreado	Es el control integrado que se verifica periódicamente para su correcta operación, actualización y evaluación sobre la efectividad de

MADUREZ	DESCRIPCIÓN
	este, con reporte al superior jerárquico correspondiente.

c. Falla por: son las prácticas por las cuales falla el control interno.

FALLA POR	DESCRIPCIÓN
Aptitud	Las medidas y prácticas no son eficientes, efectivas y oportunas. Los mecanismos de control no se adaptan a los procesos, recursos, objetivos y de fácil interpretación para los funcionarios.
Actitud	Es la forma de actuar de una persona, el comportamiento que emplea un individuo para hacer las cosas. No existe un grado de identificación por parte de los funcionarios; no demuestra iniciativa y disposición para cumplir con las directrices, reglamentaciones y ordenamientos, entre otros.
Ambos	Falla por los mecanismos utilizados (aptitud) como por los funcionarios a cargo (actitud).
Nada	No falla por nada

d. Efectividad: Son los niveles de efectividad en que está funcionando el control interno.

EFECTIVIDAD	DESCRIPCIÓN
Deficiente	Los controles son mínimos, no contribuyen a que el efecto del riesgo sea contrarrestado.
Baja	La medida de control contribuye poco a que el efecto del riesgo sea contrarrestado.
Media	La medida de control contribuye parcialmente a que el efecto del riesgo sea contrarrestado, implica el monitoreo constante del riesgo.
Alta	La medida de control contribuye a que el efecto del riesgo sea minimizado.
Óptima	La medida de control contribuye a que el efecto del riesgo sea completamente mitigado en su totalidad.

Posterior a la multiplicación de los elementos anteriores se obtiene el criterio de aceptación:

CRITERIO DE ACEPTACIÓN	DESCRIPCIÓN
Aceptable	Los riesgos que se ubiquen en este rango se consideran en nivel aceptable, serán monitoreados por el Consejo de Rectoría.
Bajo	Los riesgos que se ubiquen en este rango se consideran en nivel bajo, serán riesgos que requieren una actividad para mitigar el riesgo y deberán de ser atendidas en el corto plazo.
Moderado	Los riesgos que se ubiquen en este rango se consideran en nivel moderado, serán riesgos que requieren una actividad para mitigar el riesgo y deberán de ser atendidas en el mediano o corto plazo.
Alto	Los riesgos que se ubiquen en este rango se consideran en nivel alto, serán riesgos que requieren una actividad para mitigarlos, mismas que deberán ejecutarse y monitorearse según el comportamiento del riesgo por la persona responsable y comunicado al superior inmediato, deberán de ser atendidas en el corto plazo con el establecimiento de acciones para mitigar el impacto de su materialización.

CRITERIO DE ACEPTACIÓN	DESCRIPCIÓN
Muy Alto	Los riesgos que se ubiquen en este rango se consideran en nivel extremo, serán atendidos de manera inmediata, con prioridad Institucional. Estos requieren de una actividad para mitigarlos, deberán ser implementados y evaluados por la persona responsable y comunicado tanto al superior inmediato como al máximo jerarca deberán de ser atendidas en el corto plazo con el establecimiento de acciones para mitigar el impacto de su materialización.

El fin primordial de la gestión del riesgo, es permitir la toma de decisiones de manera oportuna ubicando a la Institución en un nivel de riesgo aceptable, sin que este afecte la consecución de los objetivos Institucionales. Una vez efectuadas las actividades de identificación y análisis de los riesgos, se debe determinar si el riesgo resultante se encuentra o no, dentro de los límites que el ITCR está dispuesto a administrar como aceptable.

4. Evaluar los riesgos: matriz de priorización, con base en el análisis de las probabilidades e impactos, cuáles serán de atención inmediata.

5. Tratar los riesgos: determinar el nivel de planificación (nivel táctico u operativo) en el cual serán administrados:

TRATAMIENTO DEL RIESGO	DESCRIPCIÓN
Evitar	Esta estrategia trata de cambiar la meta para eliminar el riesgo, por lo tanto, se espera que el ITCR detenga la ejecución de las metas.
Transferir	Traslada las consecuencias del riesgo a un tercero.
Mitigar	Reduce las posibilidades y las consecuencias de un evento, tomando acciones correctivas oportunas. Considera la determinación de nuevas alternativas para reducir el nivel de riesgo.
Aceptar	Implica la tolerancia del riesgo y sus consecuencias.

El nivel a mediano plazo de la planificación inicia a partir de la asignación de la acción en este nivel, para lo cual se deberá:

1. Dar seguimiento a la acción de respuesta al riesgo de la meta institucional asignada al Plan de mediano plazo.
2. Aplicar el Proceso de Valoración del Riesgo a los Planes de mediano plazo.
3. Elaborar el plan de acción de mediano plazo.
   En esta fase se define el responsable de ejecutar la acción de respuesta propuesta para mitigar el riesgo identificado y el plazo de ejecución.

ACCIÓN DE RESPUESTA AL RIESGO			
Acción de respuesta al riesgo	Fecha de Inicio	Fecha de Finalización	Responsable

4. Determinar si es necesario que este riesgo sea atendido en el nivel a corto plazo (operativo)

En este último nivel a corto plazo (operativo) en escalada se deberá:

1. Dar seguimiento a la acción de respuesta al riesgo de la meta institucional asignada al Plan de corto plazo.
2. Aplicar el Proceso de Valoración del Riesgo a las metas del PAO.
3. Elaborar el plan de acción de respuesta al riesgo.

Como elemento cíclico se mantiene el monitoreo y revisión de los riesgos en cada uno de los niveles de planificación y de ser necesario se realiza la actualización de los elementos del modelo citados en los puntos del 1 al 5 del primer nivel estratégico. El seguimiento se dará dos veces al año, actualizando los elementos que sean necesarios de lo operativo a lo estratégico.

Tipos de valoraciones

a. Valoración de Riesgos: estratégica-táctica y operativa

Los riesgos estratégicos, pueden carecer del precedente histórico y/u originarse fuera del sector. Las señales relacionadas con los riesgos estratégicos emergentes a menudo son débiles o intermitentes, lo cual puede hacer que sean difíciles de detectar, fáciles de descartar, y difíciles de interpretar. Las herramientas tradicionales no pueden ser confiables para localizarlos y analizarlos.

Los riesgos de la estrategia institucional podrían tener las siguientes características:

- ✓ Ser únicos para la institución dadas las características del sector educativo universitario.
- ✓ Pueden traducirse en riesgos operativos, financieros, tecnológicos, políticos u otro.
- ✓ Ser difíciles de detectar porque las probabilidades de ocurrencia son mínimas, no son amenazadoras, o bien, ya están administrados.
- ✓ Son difíciles de abordar con las metodologías establecidas.
- ✓ Es complejo cuantificarlos y rastrearlos.

b. Valoración de Riesgo-Autoevaluación

A solicitud de las dependencias, se podrá realizar el proceso de Autoevaluación y Valoración del Riesgo, identificando las debilidades del Sistema de Control Interno, generando un Plan de Mejoras al cual se le debe dar seguimiento anualmente por parte del responsable del proceso y emitir un informe del seguimiento correspondiente a la Unidad Especializada de Control Interno de la Oficina de Planificación Institucional.

c. Valoración de riesgos según Marco de Gobierno y Gestión de Tecnologías de Información

Según el Marco de Gobierno y Gestión de Tecnologías de Información establecido, se consideran en el momento de realizar la gestión de riesgos, los seis componentes del marco de gobierno, a saber:

Componente	Descripción
Alineación estratégica y operativa	Asegurar de manera óptima que lo planificado y desarrollado por TI corresponde a lo definido por la administración superior del ITCR, de tal forma que se garantice que TI contribuye a satisfacer las necesidades y expectativas institucionales
Optimización y gestión de riesgos	Producir información que apoye la toma de decisiones orientada a ubicar al ITCR en un nivel de riesgo aceptable y, así, promover, de manera razonable, el logro de los objetivos institucionales.
Optimización de recursos	Disponer óptimamente de los recursos de tecnologías de información para satisfacer las necesidades institucionales, de tal forma que se obtenga el mayor beneficio para el ITCR y la posibilidad de realizar cambios futuros
Gestión de servicios de TI	Dirigir, evaluar y dar seguimiento a las actividades que permitan garantizar la integridad de la cadena de valor del producto/servicio de TI en relación con las prácticas o procesos de las instituciones universitarias, de tal forma que sus servicios de TI funcionen eficientemente y se alineen con los objetivos del ITCR. Además, este objetivo facilita la entrega de productos y servicios de tecnologías de la información de alta calidad, logrando una mayor productividad y minimizando las interrupciones mediante la rápida resolución de consultas de usuario e incidentes
Mejora Continua	Velar por el cumplimiento de los procesos y servicios brindados por TI, así como los componentes del gobierno de TI referentes a los objetivos planteados por este y la gestión de TI.
Seguridad de la información	Propiciar de manera razonable la confidencialidad, integridad, disponibilidad, autenticidad de la información, acceso, trazabilidad y servicios utilizados en medios electrónicos, por medio de la toma de decisiones basada en riesgos para asegurar el cumplimiento de la normativa interna y externa del ITCR en materia de seguridad de TI.

Fuente: Marco de Gobierno y Gestión de Tecnologías de Información

Considerando la matriz de valoración de riesgos institucionales se determinan los posibles riesgos a partir de los componentes del marco de gobierno, para los criterios de aceptación bajo, moderado, alto y muy alto, deberán generar una acción de respuesta al riesgo.

Portafolio de Riesgos

El Portafolio de Riesgos es un insumo del proceso y define una serie de categorías de riesgo para posibilitar la creación de un lenguaje común entre los actores del sistema, en la identificación de riesgos que asume la Institución.

Se considera importante delimitar la cantidad de fuentes asociadas a una meta, así como la cantidad de eventos, vinculados por fuente; por lo tanto, se establecen los siguientes lineamientos:

a. Cada objeto de valoración (objetivo, meta, actividad, proyecto, etc.) deberá ser asociado a un máximo de tres fuentes de riesgos ubicadas en el Portafolio de Riesgos Institucional y por cada fuente de riesgos dos eventos, utilizando el juicio de experto y el conocimiento de experiencias previas.

b. El mantenimiento del Portafolio de Riesgos será una labor que estará bajo la responsabilidad de la Unidad Especializada de Control Interno, a quien los responsables deberán remitir las solicitudes de incorporación de nuevos riesgos.

Producto

- ✓ Planes de acción de respuesta al riesgo
- ✓ Informes de los resultados de la ejecución del proceso de Gestión de Riesgo
- ✓ Informes de los resultados producto de las valoraciones con aplicación del marco de gobierno y gestión de tecnologías de información.
- ✓ Informes de los resultados del seguimiento al Plan de acción de respuesta al riesgo.

Comunicación y documentación

El Informe de Gestión del Riesgo será presentado ante el Consejo de Rectoría y Consejo Institucional. Se enviará el informe en digital a la Auditoría Interna y a los responsables de ejecutar el proceso para su conocimiento e información.

SEVRI

El SEVRI-TEC será el sistema utilizado, el mismo se encuentra disponible en la página web institucional, su ingreso se realizará con el usuario y contraseña institucional. Tendrán acceso personas responsables de la Rectoría, Vicerrectorías, Direcciones de Campus Tecnológicos Locales y Centros Académicos, Direcciones de departamentos y Coordinaciones de Proyectos.

La UECI habilitará los periodos correspondientes, así como el acceso a los usuarios.