# GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

## CURSO 2022/2023

## TRABAJO FIN DE GRADO

# Implementación del modelo COSO-ERM en una Universidad Privada

# Implementation of the COSO-ERM model in a Private University

AUTORA: PAULA OCHOA BRINGAS

DIRECTOR: CRISTIAN BRINGAS PUENTE

Junio de 2023

# ÍNDICE

1. RESUMEN ..... 4
2. INTRODUCCIÓN ..... 5
3. EL CONTROL INTERNO Y LA GESTIÓN DE RIESGOS ..... 6
3.1. RELEVANCIA EN EL PANORAMA EMPRESARIAL Y EVOLUCIÓN ..... 6
3.2. EL MODELO DE LAS 3 LÍNEAS ..... 7
3.3. MARCOS DE REFERENCIA PARA LA GESTIÓN DE RIESGOS ..... 9
3.3.1 Norma ISO 31000 ..... 9
3.3.2. Metodología COSO-ERM ..... 11
4. IMPLEMENTACIÓN DE LA METODOLOGÍA COSO-ERM EN UNA UNIVERSIDAD PRIVADA. ..... 12
4.1 GOBIERNO Y CULTURA ..... 13
4.2. ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS ..... 17
4.2.1. Análisis DAFO ..... 17
4.2.2. Apetito al riesgo ..... 18
4.2.3. Formulación de objetivos y evaluación de estrategias ..... 19
4.3. COMPONENTE 3: DESEMPEÑO ..... 21
4.3.1. Identificación de riesgos ..... 22
4.3.2. Evaluación y priorización de los riesgos a nivel de cartera ..... 22
4.3.3. Respuestas ante los riesgos ..... 25
4.4. REVISIÓN Y MONITOREO ..... 26
4.5. INFORMACIÓN, COMUNICACIÓN Y REPORTE ..... 27
5. EVALUACIÓN SOBRE EL GRADO DE IMPLEMENTACIÓN DEL MODELO COSO-ERM. ..... 28
6. CONCLUSIONES ..... 30
7. BIBLIOGRAFÍA ..... 31
8. ANEXOS ..... 34

# ÍNDICE DE CUADROS

Cuadro 2.1. Estructura del Modelo de las 3 líneas ……..8

Cuadro 2.2. Comparativa de los Marcos de Referencia……..9

Cuadro 2.3. Marco de referencia COSO-ERM 2004 ..…….11

Cuadro 3.1. Cuestionario sobre el componente de "Gobierno y Cultura ……15

Cuadro 3.2. Matriz DAFO simplificada sobre la posible situación de una universidad privada ……18

Cuadro 3.3. Valores de la Probabilidad e Impacto …….. 23

Cuadro 3.4. Niveles de riesgos …….. 23

Cuadro 3.5. Mapa de riesgos inherentes de la entidad ……...23

Cuadro 3.6. Mapa de riesgos residual de la entidad …….26

Cuadro 5.1. Mapa de calor sobre el grado de implementación de la metodología COSO-ERM en la universidad……..29

# ÍNDICE DE FIGURAS

Figura 2.1. Funciones y limitaciones de la Auditoría Interna ……..8

Figura 2.2. Principios, Marco y Proceso de la Norma ISO 31000 ……10

Figura 2.3. Componentes Modelo COSO-ERM 2017 ……. 12

Figura 3.1. Organigrama de los órganos de gobierno de la universidad ……13

Figura 3.2. Apetito, tolerancia y capacidad de riesgo ……19

Figura 3.3. Clasificación de los riesgos inherentes en función del nivel de riesgo ……24

Figura 3.4. Clasificación de los riesgos residuales en función del nivel de riesgo …….26

# 1. RESUMEN

El presente trabajo tiene por objetivo mostrar, de manera simplificada pero rigurosa, el proceso de implementación del modelo COSO-ERM de gestión de riesgos sobre una entidad ficticia, más concretamente sobre una universidad privada.

En virtud del propósito establecido, y como paso previo al desarrollo del modelo, se ofrece una introducción que recoge la motivación para la realización de esta investigación, y se desarrolla un marco teórico sobre la gestión de riesgos y el control interno, a fin de contextualizar y poder comprender su utilidad y el posterior análisis realizado.

Seguidamente al marco teórico, se exponen las características propias de la universidad objeto de estudio, las cuales han sido consideradas para la aplicación del marco de referencia de gestión de riesgos seleccionado. De forma secuencial, se irán desarrollando y aplicando sobre la organización propuesta cada uno de los 5 componentes del modelo COSO-ERM (2017), y sus correspondientes principios, de tal manera que, una vez completados, se obtenga un sistema de gestión de riesgos adaptado a la organización.

Por último, se recoge una breve evaluación final sobre el grado de implantación del sistema COSO en la universidad creada, así como las conclusiones extraídas tras la elaboración del trabajo.

**Palabras clave:** Gestión de riesgos, control interno, COSO-ERM, objetivos, universidad privada, desarrollo estratégico.

# ABSTRACT

The aim of this paper is to show, in a simplified but rigorous manner, the process of implementing the COSO-ERM risk management model on a fictitious entity, more specifically on a private university.

In virtue of the established purpose, and as a previous step to the development of the model, an introduction that gathers the motivation for the realization of this research is offered, and a theoretical framework on risk management and internal control is developed, in order to contextualize and to be able to understand its usefulness and the subsequent analysis carried out.

Following the theoretical framework, the characteristics of the university under study are presented, which have been considered for the application of the selected risk management framework. Sequentially, each of the 5 components of the COSO-ERM (2017) model, and their corresponding principles, will be developed and applied to the proposed organization, so that, once completed, a risk management system adapted to the organization is obtained.

Finally, a brief final evaluation is collected on the degree of implementation of the COSO system in the created university, as well as the conclusions drawn after the preparation of the work.

**Keywords:** Risk management, internal control, COSO-ERM, objectives, private university, strategic development.

# 2. INTRODUCCIÓN

Las organizaciones, independientemente de cuál sea su actividad o su tamaño, se enfrentan diariamente a multitud de riesgos que pueden dificultar la consecución de sus objetivos (Martinez y Casares, 2011). Desde un punto de vista empresarial, el riesgo hace referencia a todos aquellos eventos que, en caso de producirse, afectarían a los resultados de una compañía, e incluso comprometerían su continuidad (Westreicher, 2021). Es por ello que la gestión de riesgos resulta altamente importante en el direccionamiento estratégico de cualquier organización, posibilitando la transformación de sus amenazas en ventajas competitivas reales y sostenibles, y fortaleciendo el control interno de la entidad (Hasper et al. 2017).

Anteriormente, la gestión de riesgos y el control interno eran una preocupación casi exclusiva del sector financiero, pero con el paso del tiempo se han ido convirtiendo en una prioridad de la alta dirección en todos los sectores industriales y de negocios (Canaza y Torres, 2018). El órgano de gobierno de toda institución, así como su cúpula directiva, debe asegurarse que la gestión del riesgo está integrada en todas las actividades y personas de la organización, y llevar un control interno efectivo que demuestre su liderazgo y compromiso. (Agudelo Zapata, 2021)

En la actualidad, debido a la globalización, el dinamismo de la industria y la intensidad de la competencia, no es suficiente con la creación de valor para los grupos de interés y la generación de una ventaja competitiva que nos permita obtener rendimientos. La clave está en su mantenimiento, y es ahí donde se pone en relevancia la utilidad de este sistema. Si la entidad no establece una clara definición de sus objetivos, presenta una estrategia inadecuada o una ejecución inapropiada, todo ello derivará en la pérdida de su ventaja competitiva, y por ende, en la reducción del valor creado, objetivo último de la organización. Por consiguiente, el control interno y la gestión de riesgos juegan un papel fundamental para resolver efectivamente estas deficiencias, y afrontar todas las incertidumbres que vayan surgiendo (tanto riesgos como oportunidades), de tal manera que se potencie la capacidad de la empresa para crear y preservar dicho valor (Instituto de Auditores Internos de España, 2021).

Considerando dicha reflexión, surge la motivación para desarrollar y aplicar un sistema de gestión de riesgos sobre una institución universitaria privada. Tanto la variabilidad del entorno en el que operan las universidades como la volatilidad de determinadas variables institucionales a las que están sometidas, ponen de manifiesto la necesidad de considerar un conjunto de riesgos en la formulación de la estrategia, su implementación y su control (Almuñias y Galarza 2016). En consecuencia, el presente trabajo abordará la implementación de un marco de referencia de gestión de riesgos, el procedimiento COSO-ERM, como determinante de la efectividad empresarial en las universidades.

# 3. EL CONTROL INTERNO Y LA GESTIÓN DE RIESGOS

Como punto de partida a la hora de analizar la aplicación de la metodología COSO-ERM de gestión de riesgos y control interno, se debe de tener claro el significado de este concepto, así como su importancia y evolución en el panorama empresarial vigente;

## 3.1. RELEVANCIA EN EL PANORAMA EMPRESARIAL Y EVOLUCIÓN

Se entiende por gestión de riesgos y control interno al conjunto de actividades, procedimientos y estructuras que promueven y optimizan la eficiencia y eficacia de las operaciones de la entidad en torno al cumplimiento de los objetivos establecidos. Lo que se pretende conseguir con la implantación de este sistema es identificar, tratar, evaluar y gestionar los riesgos, de tal manera que esta correcta gestión empresarial permita proteger a una organización de posibles pérdidas o amenazas a su funcionamiento continuo. Gracias a la utilización de este tipo de procedimientos conseguimos lo siguiente (OCDE, 2018):

- Por un lado, un sistema de control con objetivos precisos, que refleje el compromiso de la dirección con la misión y valores organizacionales, y que permita mejorar el proceso de toma de decisiones y de asignación de recursos a través de una visión integrada del negocio.
- Por otro lado, un enfoque estratégico para la gestión de riesgos que comprenda su evaluación, el tratamiento de las deficiencias y el monitoreo del sistema para garantizar su continua efectividad.

El control interno y la gestión de riesgos se estructuran dentro del Gobierno Corporativo de la organización (Orca 2022). Es responsabilidad del órgano de gobierno y de la alta dirección su aplicación dado que, en última instancia, son ellos los encargados de perseguir y salvaguardar las expectativas y propósitos de la sociedad, y por tanto, alinearlas respecto al control y la gestión de los riesgos.

Tradicionalmente, eran los “líderes” de cada área los que se encargaban de las incertidumbres propias de su campo de trabajo, bajo el denominado enfoque de gestión de riesgos en silos. Este enfoque dificultaba en gran medida el desarrollo estratégico, pues omitía el hecho de que existen riesgos que afectan a más de un área, y que muchos de ellos provienen de factores externos a la organización (Azcoti 2022). Fue así como, a consecuencia de estos problemas, las empresas acabaron adoptando un enfoque integral para la gestión del riesgo denominado *Enterprise Risk Management* (ERM). Mediante el ERM, lo que se busca es adoptar una cultura única e integrada que permita administrar las actividades de control bajo una serie de criterios homogéneos y comunes para la empresa en su totalidad (Instituto de Auditores Internos de España, 2021). Este enfoque se caracteriza principalmente por:

- Adoptar una perspectiva global y no individualizada a la hora de gestionar los riesgos y llevar a cabo el control interno.
- Estar orientado hacia la creación de valor para todos los grupos de interés de la organización.
- Analizar el impacto de los riesgos en la consecución de los objetivos y reconocer los efectos positivos de las incertidumbres (oportunidades).
- Contribuir a la consecución del ajuste estratégico y organizativo.
- Mejora la comunicación e intercambio de información.
- Ser un proceso retroalimentativo, constante y continuo que afecta a toda la organización.

De manera adicional al ERM, en 2004, se formalizó la función de la Auditoría Interna dentro de la gestión de riesgos. La Auditoría Interna se trata de una actividad objetiva e

independiente que tiene por propósito valorar y monitorear la efectividad de los controles internos y del sistema de gestión de riesgos (servicios de aseguramiento), para poder así procurar las recomendaciones necesarias para su mejora (servicio de asesoramiento). Para poder delimitar las funciones de la auditoría interna y así garantizar su objetividad e independencia, se emplea el Modelo de las 3 Líneas. Con este modelo, se consigue implementar un sistema sencillo que mejore el proceso de gestión de riesgos mediante la clara delimitación del alcance y de las competencias de cada grupo (órgano de gobierno, dirección y auditoría interna), permitiendo así garantizar su éxito continuo (Ortega, 2022).

## 3.2. EL MODELO DE LAS 3 LÍNEAS

El Modelo de las 3 líneas, actualizado por última vez en el 2020, se trata de una guía de gobernanza desarrollada por el Instituto de Auditores Internos (IAI) con el objetivo de garantizar la gestión y supervisión integral de los riesgos a través de tres niveles de actividad; las líneas. Gracias a la aplicación de este modelo basado en 6 fundamentos esenciales, las actuaciones definidas y separadas de las tres líneas de trabajo facilitan la consecución de los objetivos establecidos, y promueven un gobierno sólido y eficaz en la gestión de riesgos (*Global Institute of Internal Auditors*, 2020).

Los principios que explican su funcionamiento son los siguientes (Tien Can, 2021):

- Principio 1: Gobierno

  El gobierno de una organización debe de contar con las estructuras y procesos necesarios para asegurar la responsabilidad del consejo de administración (organismo de gobierno), la actuación de la dirección en consonancia con los intereses de la empresa y el aseguramiento y asesoramiento de un equipo de auditoría interna.
- Principio 2: Roles del Organismo de gobierno.

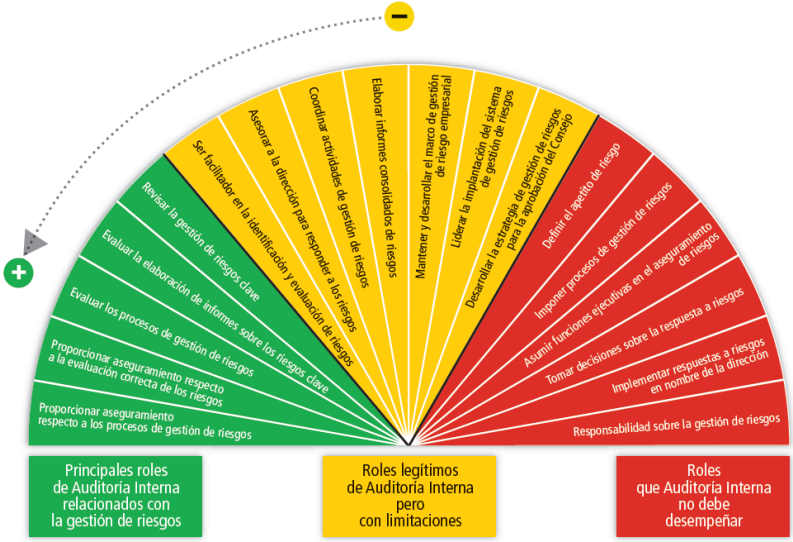
  El organismo de gobierno debe asegurarse de que se han establecido las estructuras necesarias para el correcto desarrollo de la actividad.
- Principio 3: Dirección y roles de primera y segunda línea.

  Los roles de primera y segunda línea son desempeñados por la dirección de la organización. Los primeros comprenden las actividades primarias y las de apoyo (gestión operativa) mientras que los segundos se encargan de proveer distintas funciones de gestión de riesgo (evaluación, apoyo, monitoreo…) para establecer y dar seguimiento a los controles de la primera línea. En otras palabras, los responsables de segunda línea actúan, de manera transversal, como soporte de la primera línea en la gestión de riesgos (Martínez, 2019).
- Principio 4: Roles de tercera línea

  La Auditoría Interna ocupa los roles de tercera línea. Estos son encargados de ofrecer una visión objetiva sobre el funcionamiento del gobierno y del sistema de gestión de riesgos (aseguramiento y asesoramiento). Para ello, deben de aplicar un procedimiento austero y constante, con el motivo de informar al órgano de gobierno sobre las posibles mejoras que contribuyan a la consecución de los objetivos.
- Principio 5: Independencia de tercera línea

  Los miembros de la tercera línea son totalmente independientes de la dirección, de tal manera que se garantice así la objetividad y credibilidad en sus tareas de apoyo y asesoramiento. Este principio sobre la Auditoría Interna es el que permite diferenciar el papel de los roles de segunda línea de los de tercera, puesto que, a pesar de parecer similares, los primeros si forman parte de las responsabilidades de la dirección y por tanto son dependientes de ella.

Figura 3.1. Funciones y limitaciones de la Auditoría Interna




Fuente: Instituto de Auditores Internos de España. *Auditoría Interna y Gestión de Riesgos.*

A través de la figura 3.1 se puede distinguir cómo las funciones de la tercera línea se limitan a notificar y prevenir al órgano de gobierno sin asumir responsabilidades o tomar decisiones de actuación. No obstante, existen situaciones en las que la Auditoría puede actuar asistiendo a la segunda línea o asumiendo alguna de sus responsabilidades, pero siempre con las limitaciones necesarias que garanticen su objetividad e independencia.

- Principio 6: Creando y protegiendo valor

  Finalmente, a través de la interacción y coordinación de las tres líneas, así como del consejo de gobierno, se consigue un proceso de gestión de riesgos que, basándose en hechos e información confiable, consigue potenciar y facilitar la creación de valor para las partes interesadas.

Cuadro 3.1. Estructura del Modelo de las 3 líneas


Fuente: The Institute of Internal Auditors. *El Modelo de las Tres Líneas del IAI 2020.*

Tal y como se observa a través del cuadro 3.1, mediante la implementación del Modelo de las 3 líneas se alcanza una clara definición de las estructuras, roles y responsabilidades de cada grupo, que posibilita dos aspectos esenciales; Por un lado, la alineación de las cuestiones operativas y de riesgo en la consecución de los objetivos empresariales, y, por otro lado, la existencia de una estructura para el monitoreo y evaluación de los riesgos y controles que asegure su continua eficacia.

## 3.3. MARCOS DE REFERENCIA PARA LA GESTIÓN DE RIESGOS

Se puede definir a un marco de referencia para la gestión de riesgos como la norma o procedimiento que tiene por finalidad la integración del proceso de gestión de riesgos con la estrategia corporativa de la empresa. Estos marcos de trabajo recogen las políticas, roles, responsabilidades, procesos y revisiones necesarias que se deben de llevar a cabo para poder así identificar, reaccionar y controlar los riesgos de una manera adecuada. Forman parte de la gestión institucional y han de impregnar todas sus funciones y actividades, de tal manera que se consiga así orientar todos los elementos de la empresa (equipos, personas, procedimientos…) hacia el avance en la consecución de los objetivos (*Risk and Insurance Management Society*, 2011).

En la actualidad, son cada vez más los factores que impulsan a las empresas a adoptar un sistema de gestión de riesgos. La globalización, la crisis, la creciente regulación y complejidad de la actividad, y en definitiva, la búsqueda de la maximización del beneficio para los accionistas, ponen de manifiesto la necesidad de implantar un programa ERM que contribuya a asegurar la supervivencia de la empresa.

Sin embargo, y a pesar de compartir en la mayoría de los casos los mismos incentivos, cada organización debe de escoger un marco de referencia en función de sus objetivos y de la estrategia de gestión de riesgos seleccionada para su logro (Instituto de Auditores Internos de España, 2021). El siguiente cuadro adjunto (3.2) muestra diversos estándares de ERM en función de los principales enfoques estratégicos, siendo los más utilizados la norma ISO 31000 y la metodología COSO-ERM.

Cuadro 3.2. Comparativa de los Marcos de Referencia

| Enfoque estratégico | Descripción | Marco de Referencia |
|---|---|---|
| Objetivos organizacionales | Conseguir alcanzar o superar los objetivos establecidos mediante la gestión de las incertidumbres clave y la mejora en la toma de decisiones. | • ISO 31000<br>• BS 31000<br>• COSO-ERM<br>• FERMA |
| Control y cumplimiento | Reducir o transferir los riesgos a través de actividades u objetivos de control y cumplimiento; en ocasiones basado en pérdidas pasadas, cuasi accidentes… | • OCEG “Libro Rojo”<br>• COSO-ERM |
| Requerimientos regulatorios | Necesidad de aplicar una determinada práctica o estándar y proporcionar evidencia de ello con el objetivo de cumplir con los requerimientos legales. | • Solvencia<br>• Basilea |

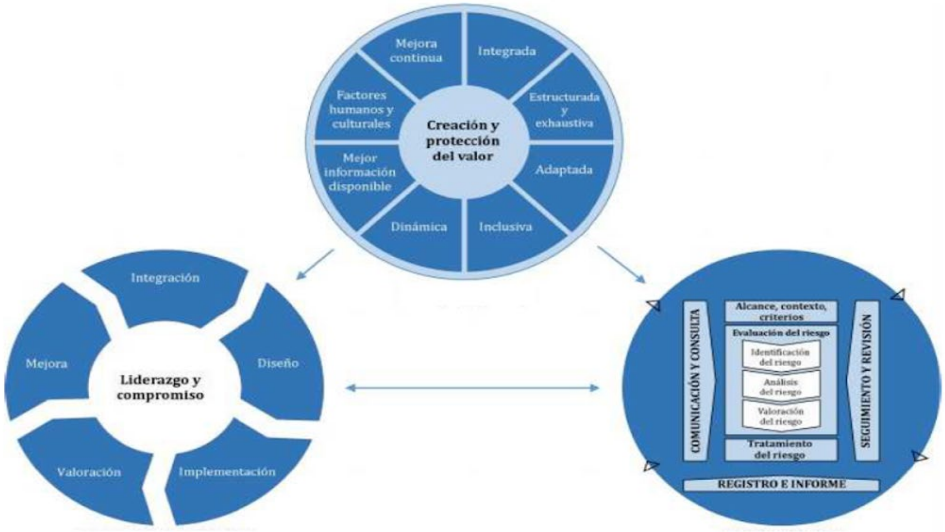
Fuente: Adaptado a partir de “*An Overview of Widely Used Risk management Standards and Guidelines*”. RIMS

### 3.3.1 Norma ISO 31000

En 2018, la Organización Internacional de Normalización (ISO) publicó la actualización de la Norma ISO 31000: Gestión de Riesgos - Directrices. A través de este estándar de gestión, se pretende ofrecer un esquema de trabajo iterativo cuya implementación permita a cualquier empresa mejorar y formalizar sus prácticas de gestión de riesgos en torno a la creación y protección de valor.

La norma ISO 31000 se incluye dentro de los estándares con enfoque estratégico de objetivos, puesto que permite a las organizaciones disponer de un proceso de control que relacione los riesgos con las recompensas, para así facilitar el logro de los resultados deseados. Es decir, si el fin último de toda organización es la creación de valor a través de la consecución de los objetivos, los riesgos deben ser valorados y tratados en la medida que se desvíen (positiva o negativamente) de dichos objetivos, y por tanto del valor esperado.

Figura 3.2. Principios, Marco y Proceso de la Norma ISO 31000




Fuente: Organización Internacional de Normalización (ISO). *Norma Internacional ISO 31000; Gestión de Riesgos – Directrices.*

A través de la figura 3.2, se distinguen las partes en las cuales se estructura la norma ISO 31000, siendo los principios, el marco de referencia y el proceso de gestión (Cobb, 2021);

- Principios: ISO 31000 enumera ocho principios necesarios para desarrollar una gestión de riesgos eficaz y eficiente en la generación de valor. En resumen, estos establecen que la gestión de riesgos tiene que ser un proceso estructurado y exhaustivo que de manera dinámica y buscando la mejora continua, utilice todos los factores y la información disponible para la creación y protección del valor. Esto implica a su vez, la adaptación del proceso a las características propias de la empresa, la integración de todas sus actividades y la participación de las partes interesadas.
- Marco de referencia: Su propósito es ayudar a las organizaciones a establecer unos mecanismos de gestión que se integren con todas sus actividades, personas y funciones. En este sentido, es fundamental el liderazgo y compromiso de las estructuras de gobierno en su función como responsables del proceso. El desarrollo del marco de referencia implica, por un lado, la integración, diseño e implementación del mismo, para posteriormente valorar su efectividad, así como las posibilidades de mejora.
- Proceso: Por último, el estándar recoge el procedimiento que deben de llevar a cabo las empresas para controlar y tratar los riesgos mediante la aplicación sistemática de una serie de políticas y prácticas. Las partes en las que queda dividido el proceso son la siguientes:
  - *Alcance, contexto y criterios*: Consiste en determinar el alcance y los criterios del sistema de gestión en base al contexto tanto interno como externo.
  - *Evaluación del riesgo*: Engloba la identificación, análisis y valoración del riesgo, indispensable para su posterior tratamiento.
  - *Tratamiento del riesgo*: Conlleva la selección e implementación de las distintas alternativas para abordar los riesgos.
  - *Revisión y seguimiento*: Comprende el monitoreo y revisión continuada del sistema a fin de asegurar su utilidad y ajuste.
  - *Comunicación y consulta*: En todas las etapas del proceso es fundamental mantener informadas a todas las partes interesadas sobre las acciones necesarias que se vayan realizando.

### 3.3.2. Metodología COSO-ERM

El modelo COSO-ERM es un marco de gestión de riesgos desarrollado por el *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) con la finalidad de ayudar a las empresas, a través de un proceso estructurado, a identificar, valorar y controlar los riesgos a los que enfrentan en el desarrollo de su actividad.

En 2004 fue publicada la primera versión de la metodología COSO para la gestión de riesgos empresariales (COSO-ERM 2004). Este modelo tuvo un gran éxito puesto que planteaba un procedimiento para la gestión de riesgos integrado en todos los procesos empresariales, con la finalidad de obtener una seguridad razonable sobre el cumplimiento de 4 objetivos: estratégicos, operativos, de reporte o comunicación y de cumplimiento. Con este propósito, la versión del 2004 se descomponía en 8 elementos clave para la administración y reducción de los riesgos, tal y como se muestra en el cuadro subsiguiente.

Cuadro 3.3. Marco de referencia COSO-ERM 2004

| | |
|---|---|
| **Ambiente Interno** | ¿Cuáles son los valores y la cultura de la organización? |
| **Establecimiento de Objetivos** | ¿Qué es lo que tratamos de conseguir? |
| **Identificación de Eventos** | ¿Qué puede hacer que no lo consigamos? |
| **Evaluación de Riesgos** | ¿Como de peligrosos son esos eventos? ¿Cuál es la probabilidad de ocurrencia? |
| **Respuesta al Riesgo** | ¿Cuáles son las opciones para evitarlos? |
| **Actividades de Control** | ¿Cómo nos aseguramos de que no ocurran? |
| **Información y Comunicación** | ¿Qué información necesitamos y como la comunicamos? |
| **Monitoreo** | ¿Cómo sabremos que hemos logrado lo que queríamos lograr? |


Fuente: Adaptado a partir de "*An Overview of Widely Used Risk management Standards and Guidelines*". RIMS

Sin embargo, a pesar de su gran utilidad, en 2017 se acabó publicando una nueva versión que respondía a las mayores exigencias del entorno y a los avances en la gestión de riesgos. De esta forma, se abandona el enfoque sobre la mitigación y la prevención de los riesgos, para dar paso a la creación de valor a través de la gestión de los mismos. En el nuevo modelo, se pone de manifiesto la creciente vinculación entre los riesgos, la estrategia y el desempeño, y la necesidad no solo de integrarlos en la gestión operativa y el control interno, sino también en la creación de valor.

En este marco actualizado diseñado por el *Committee of Sponsoring Organizations of the Treadway Commission* (2017), se recogen un conjunto de 20 principios organizados en 5 componentes del proceso de gestión de riesgos:

Figura 3.3. Componentes Modelo COSO-ERM 2017


Fuente: Gestión del Riesgo Empresarial. Integrando Estrategia y Desempeño. COSO.

- Gobierno y Cultura:
  1. Supervisión de riesgos a través del consejo de administración.
  2. Establecimiento de estructuras operativas.
  3. Definición de la cultura deseada.
  4. Compromiso con los valores clave.
  5. Atrae, desarrolla y retiene profesionales capacitados.

- Estrategia y establecimiento de Objetivos:
  6. Análisis del contexto empresarial.
  7. Definición del apetito al riesgo.
  8. Evaluación de estrategias alternativas.
  9. Formulación de objetivos de negocio.

- Desempeño:
  10. Identificación del riesgo.
  11. Evaluación de la gravedad del riesgo.
  12. Priorización de riesgos.
  13. Implementación de respuestas ante los riesgos.
  14. Visión del riesgo a nivel de cartera.

- Revisión y Monitorización:
  15. Evaluación de los cambios significativos.
  16. Revisión del riesgo y desempeño.
  17. Mejora de la gestión empresarial del riesgo.

- Información, Comunicación y Reporte:
  18. Sistemas de información y tecnología.
  19. Comunicación sobre los riesgos.
  20. Información sobre el riesgo, cultura y el desempeño.

# 4. IMPLEMENTACIÓN DE LA METODOLOGÍA COSO-ERM EN UNA UNIVERSIDAD PRIVADA.

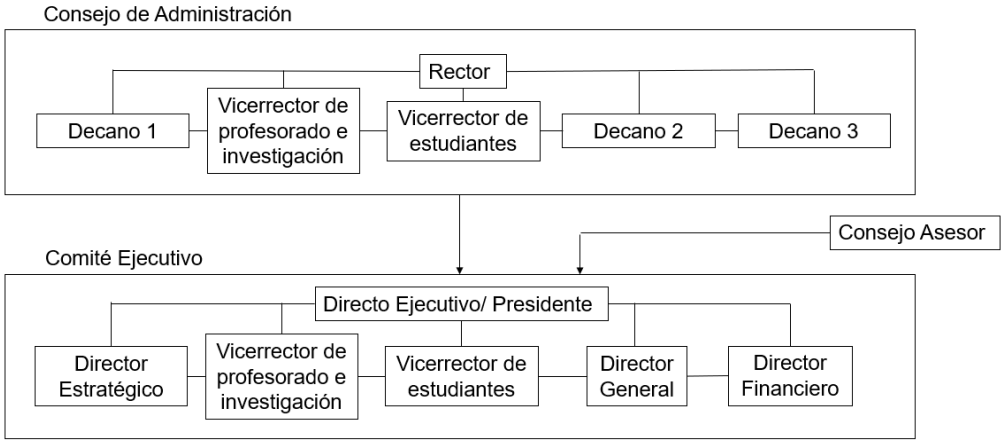
La mejor manera para comprender el funcionamiento de la metodología COSO y su utilidad en la gestión de riesgos es su aplicación práctica sobre una empresa. Para ello, se tomará como referencia una sociedad ficticia sobre la cual se irán aplicando los 20 principios del COSO-ERM con la finalidad de desarrollar, de manera simplificada pero rigurosa, un sistema que nos permita identificar, valorar y responder a los riesgos, garantizando al mismo tiempo su revisión y comunicación continua.

La empresa seleccionada para el propósito indicado es una universidad privada con la forma jurídica de Sociedad Anónima y cuya actividad CNAE (Clasificación Nacional de

Actividades Económicas) es la Educación Universitaria. Este tipo de empresa ha sido seleccionada debido a que, ante un entorno tan dinámico e incierto como el actual, las universidades, como sociedades privadas, deben de jugar un papel más activo y transformador para superar todos los inconvenientes y amenazas que puedan poner en juego su continuidad. (Almuñias y Galarza 2016))

Se supondrá que esta institución cuenta con 18 grados, 10 dobles grados y 15 posgrados, los cuales se encontrarían distribuidos en 3 facultades. En cuanto a la estructura corporativa, el Consejo de Administración de la sociedad, que queda formado por el rector, 2 vicerrectores, y los 3 decanos correspondientes a cada facultad, nombra a un Comité Ejecutivo que se encarga de desempeñar las funciones directivas en la entidad y que cuenta con los siguientes puestos: director ejecutivo/presidente, director general, director financiero, un director estratégico y los vicerrectores de profesorado e investigación y de estudiantes. Adicionalmente, la universidad contará con un Consejo Asesor que ayudará al equipo directivo asesorándolos la toma de decisiones estratégicas.

Figura 4.1. Organigrama de los órganos de gobierno de la universidad




Fuente: Elaboración propia

## 4.1 GOBIERNO Y CULTURA

El primer componente de la metodología COSO-ERM es el “Gobierno y Cultura”. El Gobierno determina la orientación de la entidad y es el encargado de poner en relieve la importancia de la gestión del riesgo en la empresa (*Committee of Sponsoring Organizations of the Treadway Commission*, 2017), así como de asegurarse y apoyar a la dirección en el establecimiento de los procedimientos necesarios para la consecución de los objetivos. La Cultura por su parte, engloba todo aquello relacionado con la misión, visión y valores éticos de la sociedad, que, en última instancia, determinan la comprensión y valoración de los riesgos.

Para evaluar la actuación de la empresa en torno al Gobierno y Cultura, se planteará un cuestionario formado por 31 preguntas (tabla 4.1). Las preguntas están estructuradas en 5 bloques distintos, correspondientes a cada uno de los principios de este componente, que son:

- Supervisión de riesgos a través del Consejo de Administración: Implica la supervisión por parte del Consejo del desempeño estratégico, así como su apoyo a la dirección en la consecución de los objetivos estratégicos y de negocio.
- Estructuras operativas: Establecimiento de las estructuras operativas necesarias para el logro de los objetivos, especialmente en la gestión de los riesgos.

- Cultura deseada: La organización define claramente su misión y visión deseada y la pone de manifiesto a la hora de abordar los riesgos.
- Compromiso con los valores clave: Demuestra el compromiso de todos los miembros y actuaciones de la entidad con los valores clave.
- Desarrollo y retención de profesionales capacitados: Emprende las acciones necesarias para disponer de un capital humano altamente cualificado y ajustado a la entidad.

Cada pregunta irá acompañada de una respuesta justificada, a la cual se le asignará una de las siguientes puntuaciones:

- 1 punto en el caso de que el requisito preguntado se cumpla y además se cuente con evidencia documental que lo corrobore.
- 0,5 puntos cuando la circunstancia inquirida se cumpla parcialmente o de una forma ambigua y no sistemática.
- 0 puntos si dicha actuación no se realiza en la empresa y se necesitan emprender acciones de mejora.

Una vez finalizado el cuestionario y habiendo obtenido la puntuación ponderada final, se ofrece una valoración sobre la actuación de la sociedad en relación con el Gobierno y la Cultura, y se señalan aquellos aspectos fundamentales en los que se debe incidir para mejorar su desempeño.

Cuadro 4.1. Cuestionario sobre el componente de "Gobierno y Cultura"

| PRINCIPIO | CUESTIONARIO | RESPUESTA | VALORACIÓN |
|---|---|---|---|
| **Supervisión de los riesgos a través del Consejo de Administración** | ¿Evalúa el consejo con regularidad que los componentes de control interno están presentes y funcionan adecuadamente? | Sí. Semanalmente deben de recibir información de los jefes departamentales y gerentes sobre las actividades de control establecidas así como de los resultados obtenido. (Ejemplo: El Departamento de Comunicacón debe presentar el reporte sobre el trafico de sitio web así como el alcance de las Redes Sociales, e informar sobre las medidas introducidas ante las desviaciones de los objetivos establecidos.) | 1 |
| | ¿Ejerce el Consejo un control efectivo sobre el cumpliento de los manuales aprobados? | Sí. Tanto gerentes como empleados deben completar de manera periódica un cuestionario sobre el cumplimiento de los procedimientos establecidos en los manuales y estos deben ser revisados por el Consejo. | 1 |
| | ¿Se reunen regularmente el Consejo de Administración y el Comité Ejecutivo? | Si. De manera mensual el órgano de gobierno debe reunirse con el Comité Directivo para realizar un seguimiento de lo efectuado hasta el momento y para asesorarlos sobre los posibles errores y las nuevas acciones a emprender. | 1 |
| | ¿Supervisa el consejo las decisiones tomadas por el Comité Ejecutivo e interviene para avisar de las posibles desviaciones observadas? | Si. Además de las reuniones mensuales, el órgano de gobierno debe de ser informado sobre cualquier decisión relevante a tomar y debe comunicar a la dirección cualquier posible riesgo que haya observado. | 1 |
| | ¿Las lineas de comunicación e información establecidas entre el Consejo y el Comité son suficientes para conocer el avance del programa de trabajo, las metas y los objetivos? | Sí. Adicionalmente a las lineas de comunicación formales, la dirección y el consejo comparten el mismo espacio de trabajo lo cual facilita y promueve la comunicación informal y continua. | 1 |
| | ¿Los controles implementados por el Consejo apoya la gestión de riesgo de los principales procesos y proyectos? | Si que tratan de mantener una comunicación constante con la direccion sobre los principales riesgos encontrados, realiza actividades de monitoreo (cuestionarios, reuniones…), y ofrece su apoyo y supervisa las acciones emprendidas. Sin embargo, no ha puesto en practica dentro de la empresa una metodología integral de gestión de riesgos para la creación de valor. (No se pone en práctica el Modelo de las 3 Líneas) | 0,5 |
| | ¿El órgano de Gobierno promueve la implantación de un marco de referencia para la gestión de riesgos con la finalidad de integrar dicho proceso con la estrategia corporativa ? | No. Ningun marco de referencia para la gestión de riesgos ha sido implantado en la empresa más allá de las actividades de control mencionadas previamente. | 0 |
| | ¿Se delega la supervisión y el asesoramiento en materia de gestión de riesgos a un consejo de auditoría interna independiente? | No existe un quipo de auditoría interna encargado del asesoramiento independiente en la gestión de riesgo. Existe un Consejo Asesor que si que puede proporcionar consejo en torno al tratamiento de los riesgos, pero este está vinculado con el Comité Directivo. | 0 |
| **Establecimiento de Estructuras Operativas** | ¿Se dispone de un manual de procedimientos actualizado y difundido en toda la organización que recoja las distintas guías de actuación necesarias para la consecucion de los objetivos? | Sí. Existe un manual que recoje de manera exhaustiva todos los procedimientos a seguir, así como un manual de aseguramiento de la calidad. Dichos documentos fueron actualizados por ultima vez en noviembre de 2022. | 1 |
| | ¿El resto de disposiciones normativas y de carácter técnico para el desempeño de las funciones están actualizadas? | No existen otro tipo de disposiciones técnicas o funcionales sobre los puestos más alla de la información suministrada por gerentes y RRHH, y la observada en el resto de trabajadores. | 0 |
| | ¿Todos los departamentos cuentan con los recursos necesarios para el correcto desarrollo de su actividad? | Se han producido algunas quejas en solicitud de recursos adicionales para el desempeño de la actividad. Ejemplo: Profesorado solicitando más salas de ordenadores o el aquipo de administración requiriendo personal de refuerzo debido al volumen de trabajo. | 0,5 |
| | ¿Se llevan a cabo actividades para verificar el cumplimiento del manual de procedimientos? | Sí. Tanto gerentes como empleados deben completar de manera periodíca un cuestionario sobre el cumplimiento con los procedimientos establecidos en los manuales. | 1 |
| | En relación a la gestión de riesgos, ¿Se dispone de un analisis DAFO de la entidad actualizado? | Si. El último analisis DAFO de la entidad fue realizado en dicembre de 2022 por el director general y aprobado por el Consejo. | 1 |
| | ¿Se examinan y valoran los posibles riesgos despredidos del analisis DAFO? | Se han analizado y planteado soluciones a los posibles riesgos desprendidos del analisis, pero de manera aislada, sin contemplar posibles alternativas y sin valorarlos en base a los objetivos de negocio y estrategicos y al nivel de riesgo tolerable. | 0,5 |
| | ¿Está identificado el riesgo aceptado o tolerable? | No se ha identificado el riesgo tolerable en base a las características y posibilidades de la entidad. | 0 |
| | ¿Se han analizado los posibles riesgos de cada departamento y se han establecido planes de contingencia al respecto? | Cada departamento trata y previene los riesgos que van surgiendo en el día a día, y consultando a la dirección ante problemas graves, pero no se desarrolla en la empresa un sistema de gestión de riesgos goblal que busque la creación de valor como es el COSO-ERM. | 0 |

| | | | |
|---|---|---|---|
| **Cultura Deseada** | ¿Están claramente definidos la misión, visión y valores? | Sí, la empresa tiene claramente definidos todos los elementos que componen su cultura. | 1 |
| | ¿Son los elementos previos coherentes en relación a los objetivos de la entidad, su dimensión y naturaleza de sus actividades? | Sí. La mision, visión y valores concuerdan con sus objetivos de excelencia académica y liderazgo en investigación, así como a su deber como formadores de futuros profesionales. | 1 |
| | ¿Existe un Código Ético que refleje la cultura deseada por la empresa? | Sí. El Codigo Ético de la Universidad recoge una clara definición tanto de la misión de la organización como de la visión a la que aspira, así como una minuciosa declaración de sus principios y valores. | 1 |
| | ¿Los valores éticos deseados son claramente comunicados y difundidos en la entidad? | Si. Existe una clara comunicación de los valores éticos compartidos en la entidad desde reclutamiento y selección de los empleados. | 1 |
| | ¿Existen una cultura en torno a la gestión de riesgos? | No. No existe en la organización una cultura que defienda una administración integral de los riesgos ya que por el momento se esta relizando de manera individual y aislada para cada actividad. | 0 |
| **Compromiso con los Valores Clave** | Adicionalmente a la comunicación de los valores éticos, ¿van acompañados de una orientación explícita sobre lo que es correcto o incorrecto? (Desarrollo del Código Ético) | Sí. En el Codigo Ético de la entidad puede ser consultado en detalle la explicación y orientación precisa de cada uno de los valores de la empresa. Adicionalmente, el equipo de RRHH es el encargado de formar a los trabajadores en dicho valores deseados. | 1 |
| | ¿Los órganos de gobierno se aseguran del cumplimiento efectivo de lo establecido en el Código Ético de la entidad? | Sí. Al igual que ocurria con el Manual de Procedimientos, los órganos de Gobierno deben de recibir periodicamente un informe sobre el grado de cumplimiento del Código, asi como de las posibles denucias e infracciones cometidas. | 1 |
| | ¿Existe un mecanismo que anime a los empleados a presentar denuncias por sospechas de violaciones y se toman decisiones disciplinarias contra empleados que conscientemente optan por no informar de ellas? (Falta de canal de denuncias) | Sí. La organización dispone de una canal de denuncias digital que permite a los empleados y alumnos informar de manera confidencial sobre las infracciones cometidas. Adicionalmente, los empleados que no hayan informado de las infracciones presenciadas, serán sancionados de la misma manera que el infractor. | 1 |
| | ¿Existe algún procedimiento y órgano que actúe contra el dolo que se haya podido cometer? (Posible falta de procedimiento sancionador y Comité de Ética) | Sí. Existe un Comité de Etica cuya labor es juzgar e imponer sanciones a las personas acusadas. | 1 |
| | ¿Se realizan acciones para fomentar la cultura de gestión de riesgos? | No. Debido a la ausencia de una marco de referencia para la gestión de riesgos, no hay tampoco una cultura en torno a dicha actividad y por tanto no se han emprendido acciones para poner en relevancia su determinación en la creación de valor empresarial. | 0 |
| **Desarrollo y Retención de Profesionales Cpacitados** | ¿Los perfiles y descripciones de los puestos, así como los requisitos de contratación están alineados con los objetivos estratégicos y de negocio? | Sí. La descripciones de los puestos son claras y ajustadas a la realidad y el peronal de contratación recibe la información necesaria para contratar a la personas más adecuadas para cada puesto. | 1 |
| | ¿Las competencias de los empleados de la entidad reflejan los conocimientos y habilidades necesarios para realizar las tareas asignadas y alcanzar los fines deseados? | Sí. Los trabajadores son contratados en base a los conocimientos y habilidades necesarias en el puesto y además, de manera frecuente, son formados en las competencias adicionales para el correcto desempeño de su actividad. | 1 |
| | ¿Existe un plan de carrera profesional para desarrollar y retener al personal competente? | Sí. Cada aréa de trabajo dispone un plan de carrera propio ajustado a las posibilidades de ascenso. | 1 |
| | ¿Se realizan actividades que fomentan la integración del personal y favorecen el clima laboral? | Sí. Desde la organización se promuven de manera constante actividades de *team building* tales como eventos internos, actividades deportivas, scape rooms… | 1 |
| | ¿Reciben los trabajadores concienciación y formación sobre la prevención y gestión de riesgos? | No. No se han desarrollado acciones ni formaciones sobre la gestión de riesgos en la empresa. | 0 |
| | | PUNTUACIÓN TOTAL (Promedio)= | 0,693548387 |
| | | GRADO DE CUMPLIMIENTO DEL COMPONENTE "GOBIERNO Y CULTURA" | MEDIO |

Fuente: Elaboración Propia a partir de "Cuestionario de autoevaluación del control interno" (Instituto Nacional de Estadística y Geografía)y de "*Compliance risk management: Applying the COSO ERM framework"* (Society of Corporate Compliance and Ethics & Health Care Compliance Association)

A partir del cuestionario realizado, esta Universidad obtiene como puntuación final un 0,69. Esta puntuación implica que, de acuerdo a los principios recogidos en el bloque de “Gobierno y Cultura", la institución presenta un grado medio de cumplimiento de los mismos. De manera general y en base a las respuestas proporcionadas, es posible verificar que el principal punto débil de la sociedad y la razón por la cual la puntuación es ligeramente baja, es la ausencia de un marco de referencia para la gestión de los riesgos empresariales.

A pesar de las fortalezas observadas, como los controles internos y seguimientos ejercidos por el Consejo, su comunicación continua con el Comité Directivo, el compromiso con una cultura acorde a los objetivos estratégicos y de negocio o el desarrollo y retención de un personal altamente capacitado, la empresa presenta una clara deficiencia en torno a los riesgos. Es por ello que, para este caso concreto, sería recomendable la introducción de una metodología de gestión de riesgos como puede ser el COSO-ERM. Con su introducción, se potenciarían los aspectos positivos hasta ahora alcanzados, hacia una visión integral de los riesgos y del control interno que permitiese involucrar esta actividad dentro de la cultura y del desarrollo estratégico de la empresa.

Con esto no solo se conseguirían alcanzar los objetivos y metas aspirados de una manera más eficaz y eficiente, sino que también se podría poner solución a los problemas existentes. Por ejemplo, se señalaba en el cuestionario el descontento de determinados grupos ante la falta de recursos necesarios. Con la introducción de un nuevo sistema de gestión, la entidad podría anticipar dichos riesgos e introducir medidas para prevenirlos.

Por lo tanto, en los apartados siguientes, se desarrollarán el resto de componentes del programa COSO-ERM, para poder así implementar en este tipo de empresa una metodología eficaz para la gestión del riesgo.

## 4.2. ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS

Toda organización debe de contar con una estrategia planificada que le permita alinear todas sus acciones, personas y equipos hacia la consecución de los objetivos propuestos. Sin embargo, las frecuentes modificaciones en el contexto externo e interno, tales como los movimientos de los competidores, los cambios en las necesidades de los clientes o incluso las oportunidades de mejora, afectarán en su capacidad para alcanzar las metas programadas. Es por ello que, la gestión del riesgo empresarial, tiene que ser incluida en la definición y despliegue de la estratégica, con el propósito de identificar los eventos potenciales que puedan afectar a la entidad, prevenir las amenazas, ofrecer una seguridad razonable sobre el cumplimiento de su misión y en definitiva, producir un valor superior. (Canaza y Torres 2018)

En virtud de esta idea fundamental, se procederá a realizar, en el presente apartado, un análisis del entorno empresarial, con el propósito de conocer los efectos potenciales del contexto sobre la empresa y considerarlos para la formulación de una serie objetivos de negocio que se pretenden alcanzar. Posteriormente se evaluarán aquellas posibles estrategias necesarias para su cumplimento en base al apetito al riesgo que se está dispuesto a asumir.

### 4.2.1. Análisis DAFO

Como paso previo a la formulación de los objetivos, una empresa debe conocer los factores que condicionan y/o condicionarán su desempeño. En ese sentido, se realizará un análisis DAFO a través del cual se obtendrán las debilidades y fortalezas vinculadas al funcionamiento interno de la organización, y las amenazas y oportunidades del

entorno en el que opera. Esta herramienta resulta muy útil en la gestión de riesgos puesto que, de manera sencilla, nos permite extraer resultados que faciliten la toma de decisiones y la elaboración de un plan estratégico. (Speth 2016)

A continuación, se ofrece una matriz DAFO simplificada sobre la posible situación de una universidad privada, de tal manera, que, a partir de las conclusiones extraídas sobre la misma, se formulen una serie de objetivos de negocio posibles para este tipo de entidad.

Cuadro 4.2. Matriz DAFO simplificada sobre la posible situación de una universidad privada.

| Debilidades | Amenazas |
|---|---|
| • Bajo reconocimiento externo (nacional e internacional)<br>• Falta de posicionamiento en redes (poco alcance)<br>• Elevados costes de mantenimiento del inmovilizado por envejecimiento.<br>• Carencia de personal en administración.<br>• Ausencia de oferta de títulos oficiales en inglés.<br>• Escasez en la oferta de programas de intercambio.<br>• Bajas tasas de rendimiento académico y altas tasas de abandono.<br>• Planes de estudios rígidos y demasiado teóricos.<br>• Escasa atracción del talento. | • Percepción de menores niveles de exigencia y calidad en las universidades privadas.<br>• Inflación generalizada en España que hace crecer el gasto corriente.<br>• Subida de los tipos de interés.<br>• Alta competencia en el segmento de enseñanza superior universitaria, con exceso de oferta en el número de títulos de grado y posgrado.<br>• Tendencia decreciente en la natalidad. |
| **Fortalezas** | **Oportunidades** |
| • Gran oferta de prácticas externas remuneradas en empresas de la región.<br>• Amplio programa de becas al estudio.<br>• Aumento del reconocimiento de la labor investigadora del PDI (personal docente e investigador)<br>• Precios de grado y posgrado competitivos.<br>• No existe masificación en las aulas.<br>• Colaboración constante con organismos y entes públicos, asociaciones empresariales y colegios profesionales.<br>• Disponibilidad de recursos financieros. | • Exigencias crecientes en los requisitos mínimos de investigación para las universidades privadas.<br>• Demanda creciente de títulos de modalidad online y semipresencial que genera una nueva oportunidad de negocio.<br>• Ausencia de otra universidad privada en la región. |

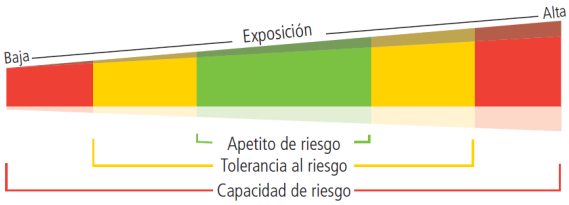
Fuente: Elaboración propia

### 4.2.2. Apetito al riesgo

Todas las organizaciones deben asumir riesgos para poder crecer. Sin embargo, el Consejo de Administración y la alta dirección, además de gestionar dichos riesgos, deben de valorar si están dispuestos a afrontarlos o no, y es ahí donde aparece la delimitación del apetito al riesgo. El apetito al riesgo es la “cantidad” de riesgo que la entidad está dispuesta a aceptar en su búsqueda de valor y que, por ende, influencia la forma en que la entidad opera (Ambrosone, 2007). Unido al apetito, se determina la tolerancia al riesgo; el umbral de alerta utilizado para evitar que la entidad llegue al nivel

que pondría en peligro la continuidad del negocio, conocido como la capacidad de riesgo (Conejos Merita, 2018).

Figura 4.2. Apetito, tolerancia y capacidad de riesgo.




Fuente: Instituto de Auditores Internos. *Definición e implantación de apetito de riesgo*.

En determinadas sociedades, el apetito al riesgo permite asegurar el cumplimiento de ciertas normativas o recomendaciones de buen gobierno. Sin embargo, su utilidad va más allá, siendo una pieza fundamental de la cultura de la organización, que cohesiona a las personas, los procesos y los recursos que la integran. (Instituto de Auditores Internos, 2013). La definición del apetito al riesgo facilita, entre otras cosas: la toma de decisiones, la alineación de los objetivos con la misión y visión, la evaluación de las estrategias y los riesgos, la asignación de los recursos, etc.

No existe un apetito al riesgo genérico que pueda ser utilizado por todas las empresas, puesto que cada una de ellas realiza sus funciones en contextos diferentes y con objetivos dispares, y por tanto, este debe ser adaptado a sus características propias. (Deloitte, 2020)

En el presente caso de estudio, el apetito al riesgo deseado se definirá en términos cuantitativos y cualitativos, en relación al posible impacto de los riesgos en la consecución de la misión y visión deseada. Para ello, se emplea un enfoque descendente (*Topdown*), con el cual, el Consejo de Administración define el apetito desde el más alto nivel organizativo, alineado con los objetivos estratégicos, que posteriormente va descendiendo por el resto de la organización para alinear la gestión de riesgos de todas las áreas (Instituto de Auditores Internos, 2013).

La cultura de la universidad hacia el riesgo siempre se ha inclinado hacia una vertiente más conservadora y prudente. Sin embargo, en estos momentos, está dispuesta a asumir más riesgos ya que tiene el propósito de aumentar su base de estudiantes y mejorar sus servicios y su reputación, y además, cuenta con una situación financiera favorable. Por ello, se define un apetito al riesgo medio, es decir, se podrán aceptar ciertos riesgos siempre y cuando su asunción potencie su labor como educadores de calidad superior (misión) y su búsqueda de la excelencia académica y la innovación educativa (visión).

En términos cuantitativos, este apetito al riesgo medio implicaría aceptar aquellos riesgos cuya valoración, en función de la probabilidad de ocurrencia e impacto sobre la empresa, sea inferior a los 9 puntos, lo cual puede ser más tarde observado mediante el mapa de riesgos. Además, cada área operativa podrá adaptar dicho apetito al riesgo siempre y cuando no sobrepase los límites tolerables.

### 4.2.3. Formulación de objetivos y evaluación de estrategias

Una vez analizada la situación actual de la empresa y habiendo identificado sus factores condicionantes, se procede a la formulación de una serie de objetivos operativos desprendidos de dicha valoración. El propósito de estos objetivos es impulsar los esfuerzos de la organización hacia el logro de la estrategia corporativa (Pursell, 2023).

Cada uno de ellos, irá acompañado de una estrategia factible para su logro. Gracias al desarrollo de dichas estrategias, se consigue planificar correctamente las acciones que se deberán de llevar a cabo para obtener los resultados deseados, y, además, facilitarán la identificación de los posibles riesgos que puede entrañar su puesta en funcionamiento.

1. Debido a las bajas tasas de rendimiento académico presentadas por el alumnado y las altas tasas de abandono, posiblemente causadas por la desmotivación de los estudiantes, se considera necesaria la introducción y desarrollo de nuevos modelos docentes, avanzados en tecnologías y en nuevas tendencias pedagógicas. Con ello, lo que se pretende conseguir es una nueva forma de aprendizaje activo, participativo y personalizado, a través del cual los individuos adquieran una formación que se adecue a las demandas profesionales del mercado laboral.
   Por ello, se plantea como estrategia para su logro, la implementación de dos metodologías activas de docencia apoyadas en las TIC (Tecnologías de Información y Comunicación): el aprendizaje basado en problemas (ABP) y el análisis de casos. Con estos métodos complementarios a las técnicas de enseñanza actuales, lo que se consigue son unos alumnos más autónomos, responsables y concienciados con su aprendizaje. Con el aprendizaje basado en problemas, el estudiante se enfrentaría a ciertas situaciones asociadas a su profesión como punto de partida para la adquisición de los conocimientos (Diez Barriga, 2005), mientras que con el análisis de casos se estudiará una situación, real o ficticia, pero factible, que recree las condiciones del medio laboral del futuro profesional. (Silva y Maturana, 2017).

2. Cada vez es mayor la competencia en el sector de la enseñanza universitaria privada, habiéndose multiplicado por 5 desde el inicio del siglo (BBVA, 2017) y acogiendo en la actualidad al 17,8% del alumnado en España (Carabante, 2023). Surge entonces así la necesidad de ofrecer a la sociedad un nuevo servicio que diferencie a la organización de sus competidores. A causa de la pandemia ha aparecido una nueva forma de enseñanza que aún no está siendo explotada y que genera un nuevo objetivo para la entidad: Ofrecer títulos de modalidad online ante su creciente demanda.
   La estrategia planteada para su logro constaría de los siguientes pasos:
   - Realizar un análisis de la viabilidad del programa en relación con la demanda del mercado, la capacidad de la organización y el presupuesto necesario.
   - Identificar las titulaciones de mayor demanda y aquellas más viables para ser impartidas de forma online.
   - Diseñar un plan de acción que incluya la formación del personal, la adquisición de tecnología y el desarrollo de plataformas de enseñanza virtual.
   - Llevar a cabo una campaña promocional que atraiga a estudiantes potenciales.

3. Tanto del análisis DAFO como del Cuestionario sobre el “Gobierno y Cultura” se desprende la carencia de personal en el área de administración. En estos momentos, la mayoría de los procedimientos administrativos se registran de manera manual, lo que produce un volumen excesivo de trabajo que estos empleados no son capaces de atender. Por ello, aparece la necesidad de automatizar y digitalizar muchos de los procesos administrativos, de tal manera que se reduzca la cantidad de tareas a realizar.
   En base al objetivo propuesto, se le encargará a una empresa el desarrollo de un software para la gestión administrativa de la universidad, capaz de integrar y controlar en una misma base de datos toda la información relacionada con el centro y con su actividad diaria, tanto interna como externa, como pueden ser las

matriculaciones, la facturación, los datos académicos, comunicaciones, becas, control de las instalaciones, etc. Dicho sistema será introducido en la entidad en base a sus necesidades y de manera progresiva, con el propósito de asegurar su correcto funcionamiento. Además, el personal recibirá una formación rigurosa sobre su manejo.

4. La falta de posicionamiento en redes sociales y su bajo reconocimiento externo ha propiciado la aparición de un nuevo objetivo para la sociedad; El desarrollo de un plan de comunicación online mediante el cual pueda exponer sus fortalezas (grandes labores investigadoras, oferta de prácticas externas remuneradas, precios competitivos o amplios programa de becas al estudio) y ampliar su alcance. De esta forma, lo que se pretende conseguir es aumentar el número de alumnos matriculados y la atracción del talento.
   La planificación a seguir para su desarrollo constaría de los siguientes pasos (Pérez, 2018):
   - Análisis de los recursos de comunicación actuales de la entidad, así como los de la competencia, y de la situación del mercado, previo a la formulación de las metas a conseguir (Tur-Viñes y Monserrat-Gauch, 2014).
   - Selección de los canales de comunicación y del público objetivo.
   - Diseño de un mensaje claro y conciso.
   - Valoración de los recursos y elaboración de un plan de ejecución.
   - Medición.

5. Ante la disponibilidad de recursos financieros, el último objetivo seleccionado es la renovación del inmovilizado e instalaciones de la universidad con el propósito de reducir los elevados costes de mantenimiento y conseguir hacerla más atractiva para los posibles estudiantes. Para lograrlo, se propone la selección de un equipo de trabajo adecuado, que, de manera progresiva y planificada, y en base al presupuesto establecido, vaya realizando pequeñas obras y modificaciones que no interfieran en la actividad docente.

Los objetivos y estrategias expuestos han sido seleccionados al constituir acciones concretas para convertir la universidad en una institución líder en la excelencia académica, la innovación educativa y la formación integral de profesionales (visión). En el siguiente apartado, se identificarán y evaluarán los principales riesgos asociados a cada objetivo, en base al apetito establecido y a su impacto potencial en el perfil de riesgos deseado. De esta manera, se podrán establecer prioridades respecto al tratamiento de los riesgos, e incluso prioridades respecto a la consecución de los objetivos.

## 4.3. COMPONENTE 3: DESEMPEÑO

De acuerdo al *Committee of Sponsoring Organizations of the Treadway Commission* (2017), el tercer componente de la metodología COSO-ERM implica la identificación y evaluación de los riesgos que puedan afectar a la consecución de los objetivos, para poder así priorizarlos, en función de su gravedad en el contexto del apetito al riesgo, e implementar las respuestas adecuadas.

En el presente caso de estudio, se identificarán los riesgos asociados a los objetivos previamente formulados, los cuales serán evaluados a nivel de cartera, es decir, de manera agregada para el conjunto de la entidad. Posteriormente, se priorizarán los riesgos como base para la selección de respuestas a adoptar.

### 4.3.1. Identificación de riesgos

A partir de los objetivos expuestos, es posible distinguir los siguientes riesgos:

1. Falta de capacitación para el desarrollo de los nuevos métodos de enseñanza por parte del personal docente actual: Los profesores pueden no estar debidamente capacitados para implementar las nuevas metodologías pedagógicas de manera efectiva, lo cual podría generar la desmotivación y frustración del alumnado. Esta situación causaría el fracaso de los nuevos sistemas en su propósito por mejorar el rendimiento académico y reducir el abandono.
2. Incumplimiento del diseño curricular y de los requisitos docentes de las titulaciones recogidos por la normativa vigente aplicable: El ajuste de los programas formativos y planes de estudio a causa de la introducción de los nuevos modelos pedagógicos, puede propiciar la violación de los estándares, normas y regulaciones establecidos en la legislación actual para la enseñanza y la calidad educativa.
3. Interrupción de la conexión a Internet o fallo de la plataforma: La enseñanza online depende de la tecnología y de la conectividad a Internet. Por ello, si se produce una interrupción del servicio de Internet o un fallo en las plataformas digitales de docencia empleadas (ej. aula virtual) se puede interrumpir el aprendizaje y la enseñanza.
4. Incumplimiento de los requisitos de evaluación recogidos por la normativa actual: La selección de los métodos de evaluación en la enseñanza online resulta más difícil que en el entorno de enseñanza tradicional. Por ello, existe la posibilidad de que, al tratar de aplicar un sistema de evaluación justo y preciso, se incumpla con la legislación vigente en relación a este aspecto.
5. Ciberataque al sistema informático de la entidad: El software puede contener vulnerabilidades que permitan a posibles atacantes acceder a él, para bloquearlo, dañarlo o alterar datos críticos. Este tipo de ataque derivaría en la pérdida o alteración parcial o total de la información.
6. Pérdida de control sobre el mensaje del plan de comunicación: La información que se comparte puede ser malinterpretada o distorsionada por los medios de comunicación o el público, lo que puede dañar la reputación de la empresa. Al no transmitir efectivamente sus fortalezas y logros educativos, la empresa tendría dificultades para atraer y retener estudiantes, así como para establecer asociaciones externas.
7. Costes excesivos en la renovación de las instalaciones e inmovilizado: La renovación de las instalaciones y los posibles retrasos y dificultades asociadas al desarrollo de las obras pueden resultar en costos imprevistos y gastos adicionales que afectarían al presupuesto de la universidad. Todo ello, unido a un contexto de inflación generalizada en España, que aumenta el gasto necesario para llevar a cabo las renovaciones (sobrecostos en la ejecución), y de subida de los tipos de interés, que eleva el coste de la financiación.
8. Contratación de personal para el desarrollo del plan de comunicación: Es muy probable que sea necesario contratar a una o dos personas para el desarrollo de esta estrategia, ya que puede que con el personal actual a su cargo no sea suficiente.

### 4.3.2. Evaluación y priorización de los riesgos a nivel de cartera

Para evaluar los riesgos identificados se elaborará una matriz que clasificará los riesgos en función de su probabilidad de ocurrencia y del impacto o daño potencial sobre la empresa. La matriz contará con 4 valoraciones posibles, tanto para la probabilidad como para el impacto, tal y como se muestra en el siguiente cuadro:

Cuadro 4.3. Valores de la Probabilidad e Impacto.

| Probabilidad | | | Impacto | | |
|---|---|---|---|---|---|
| Valor | Escala | Concepto | Valor | Escala | Concepto |
| 1 | Dificil | Su ocurrencia sería un caso excepcional (Probabilidad <20%) | 1 | Leve | Pérdida de entre 0 y 30000€ |
| 2 | Poco probable | La probabilidad es baja pero factible (20-49%) | 2 | Moderado | Pérdida de entre 30.001 y 90.000€ |
| 3 | Probable | La probabilidad de ocurrencia es alta (50-80%). Ha ocurrido alguna vez con anterioridad. | 3 | Fuerte | Pérdida de entre 90.001 y 180.000€ |
| 4 | Muy probable | Lo más seguro es que ocurra (> 80% de probabilidad). / Ya ha ocurrido varias veces con anterioridad | 4 | Muy fuerte | Pérdida > a 180.000€ |

Fuente: Elaboración propia

Los riesgos obtendrán de esta forma una puntuación en función de su nivel de amenaza (alto, medio-alto, medio-bajo, bajo), la cual irá del 1 al 16 y se calculará multiplicando el valor de la probabilidad por el del impacto.

Cuadro 4.4. Niveles de riesgos

| Nivel de Riesgo | Puntuación |
|---|---|
| Alto | 12, 16 |
| Medio-Alto | 8, 9 |
| Medio-Bajo | 4, 6 |
| Bajo | 1, 2, 3 |

Fuente: Elaboración propia

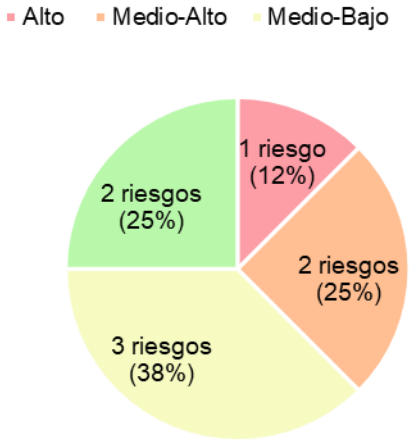
Gracias a la clasificación obtenida, los riesgos podrán ser posteriormente valorados según su peligrosidad, facilitando así el establecimiento de prioridades para la posterior implementación de respuestas.

Cuadro 4.5. Mapa de riesgos inherentes de la entidad.

| | | | | |
|---|---|---|---|---|
| 4-Muy probable | Riesgo 3 | Riesgo 8 | | |
| 3-Probable | | | Riesgo 6 | Riesgo 7 |
| 2-Poco probable | | | Riesgo 1 | |
| 1-Dificil | Riesgo 2 y 4 | | | Riesgo 5 |
| Probabilidad de Ocurrencia/ Impacto | 1-Leve | 2-Moderado | 3-Fuerte | 4-Muy fuerte |
| | 0-30.000€ | 30.001-90.000€ | 90.001-180.000€ | >180.000€ |

Fuente: Elaboración propia

Figura 4.3. Clasificación de los riesgos inherentes en función del nivel de riesgo




Fuente: Elaboración propia

El cuadro 4.5 recoge el mapa de riesgos inherentes (aquellos sobre los cuales no han sido aplicadas medidas de control) asociado a la entidad objeto de estudio, mientras que la figura 4.3 ofrece una clasificación según el nivel de riesgo. A través de su análisis, es posible extraer las siguientes conclusiones:

- Los dos riesgos por incumplimiento de la normativa, ya sea el de los requisitos docentes o el de los requisitos de evaluación (riesgos 2 y 4), tendrían un impacto moderado, al ir acompañados de sanciones de entre 15.000-25.000€. Además, presentan una probabilidad difícil puesto que estos requisitos siempre son formulados atendiendo a la legislación existente, por lo que su incumplimiento sería una situación totalmente excepcional. Es por ello que presentan un nivel de riesgo bajo y no necesitan ser atendidos.
- Existen 3 riesgos de nivel medio-bajo:
    - El riesgo 1 representa la falta de capacitación del personal docente para el desarrollo de las nuevas metodologías pedagógicas. Se trata de un riesgo poco probable, puesto que la Universidad cuenta con profesionales altamente cualificados, pero que nunca han trabajado con este tipo de técnicas, lo que hace factible su ocurrencia. Asimismo, iría acompañado de un fuerte daño a la entidad, al ocasionar el abandono de entre 25-35 alumnos, lo cual, en base a unos 5.000€ por matrícula, implicaría una pérdida de entre 125.000-175.000€. En este sentido, el riesgo 1 sería el primer riesgo medio-bajo en atender.
    - El riesgo 3, fallo de la conexión a Internet o de la plataforma de enseñanza, tiene una probabilidad de ocurrencia muy alta, ya que suele producirse una o dos veces al año, pero sin embargo su impacto es prácticamente nulo, por lo que sería el último riesgo en atender dentro de esta categoría.
    - La probabilidad del riesgo 5, el ciberataque, es muy baja (< 5%) al tratarse de un software altamente protegido. En cambio, el impacto es muy fuerte, pues en caso de producirse podría llegar a acarrear el cierre de la entidad. Por ello, sería el segundo riesgo de la categoría en ser tratado.
- Dentro de la categoría medio-alta se sitúan dos riesgos; El más peligroso de ellos es el riesgo 6, pérdida de control sobre el mensaje del plan de comunicación. Esto es causado por su probabilidad significativa, al ser el mensaje fácilmente malinterpretado o modificado por la opinión pública, y por su fuerte impacto, al poder provocar la falta de atracción de unos 30 alumnos (=175.000€). El riesgo 8, la contratación de personal, presenta una puntuación de 8, principalmente debido a ser una necesidad altamente probable. En cambio, el daño sobre la entidad no sería

elevado, al suponer un gasto de unos 40.000€ en salarios y el cual sería compensado con la efectividad del plan de comunicación. Por ello, se priorizará el tratamiento del riesgo 6, cuya elusión podría compensar el coste del riesgo 8.

- El único riesgo alto identificado es el posible gasto excesivo de renovación del inmovilizado y de las instalaciones. Esta clasificación responde a una probabilidad de 3 puntos, al ser significativamente verosímil la prolongación de las obras y la consecuente elevación de los costes, y a un impacto de 4 puntos, puesto que en el caso de que se produzca podría involucrar un gasto superior a los 180.000€. En consecuencia, al superar los 9 puntos definidos por el apetito al riesgo y poder dificultar el desarrollo del resto de objetivos ante la escasez de presupuesto derivada, la consecución de este fin será pospuesta para otro momento.

Finalmente, el orden para el tratamiento de los riesgos quedaría de la siguiente forma:
1. Pérdida de control sobre el mensaje del plan de comunicación.
2. Falta de capacitación para el desarrollo de los nuevos métodos de enseñanza por parte del personal docente actual.
3. Ciberataque al sistema informático de la entidad.
4. Interrupción de la conexión a Internet o fallo de la plataforma.

### 4.3.3. Respuestas ante los riesgos

Una vez evaluados y valorados los riesgos, se procede a exponer las respuestas necesarias para su tratamiento, siguiendo el orden de prioridad planteado en el apartado anterior:

- Debido a la complejidad del riesgo de pérdida de control sobre el mensaje en la comunicación, se consideran las siguientes estrategias:
    - Asegurarse que los mensajes a transmitir sean claros, coherentes y alineados con los objetivos, y no sean contradictorios entre los distintos medios de comunicación.
    - Establecer un tono y estilo de comunicación acorde a los valores de la entidad y al público objetivo, para evitar así la confusión.
    - Monitorear y medir las respuestas y reacciones generadas, con el propósito de realizar los cambios que sean necesarios.
    - Mantener una comunicación constante y activa con la audiencia, de tal manera que se puedan corregir posibles tergiversaciones del mensaje.

  Con la aplicación de estas medidas, se reduciría la probabilidad de ocurrencia e impacto del suceso, al ejercer un seguimiento continuo del mensaje y tratar de poner solución a las posibles desviaciones.

- Desarrollar un plan de capacitación en las nuevas metodologías de docencia, que incluya sesiones específicas, talleres, cursos en línea y otras actividades formativas, que serán realizadas por el personal dentro de su horario de trabajo. Para medir el impacto de la capacitación en el desempeño se realizarán evaluaciones periódicas que permitirán realizar los ajustes necesarios en el programa, y además, las 3 personas con mejores evaluaciones recibirán un premio en especie con el propósito de incentivar así al personal. Bajo estas circunstancias, se reduciría la probabilidad de ocurrencia, y, además, en caso de producirse, serían menos los profesores incapacitados y por ende menor el número de alumnos decepcionados y el coste asociado a su abandono.

- Adquirir discos duros externos con una alta capacidad de almacenaje, en los cuales cada día se recoja una copia de seguridad de la información acumulada hasta ese momento. De esta forma, si se produjese el ciberataque ataque, se reduciría el

impacto al mínimo nivel, ya que solo sería necesario volver a registrar la información añadida con posterioridad a la última copia de seguridad.

- Disponer de una red de Internet alternativa a la cual conectarse en caso de fallo de la principal, y promover entre alumnos y profesores la descarga de los contenidos para no depender así de la plataforma digital. Siguiendo esta línea, se reduce la probabilidad del riesgo a la mitad, pasando de muy probable a poco probable.

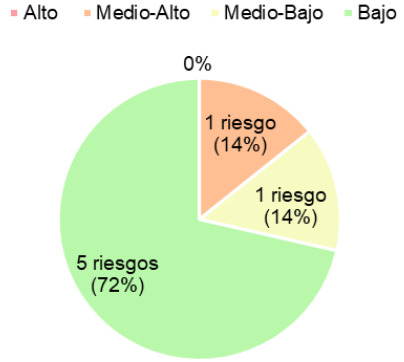
En definitiva, tras la correcta aplicación de las medidas definidas y considerando la postergación del objetivo de renovación de las instalaciones, se reduciría el nivel de riesgo soportado por la organización y se obtendría el siguiente mapa de riesgos residuales y su correspondiente clasificación:

Cuadro 4.6. Mapa de riesgos residuales de la entidad.

| | | | | |
|---|---|---|---|---|
| 4-Muy probable | | Riesgo 8 | | |
| 3-Probable | | | | Riesgo 7 |
| 2-Poco probable | Riesgo 3 | Riesgo 6 | | |
| 1-Dificil | Riesgo 2, 4 y 5 | Riesgo 1 | | |
| Probabilidad de Ocurrencia/ Impacto | 1-Leve | 2-Moderado | 3-Fuerte | 4-Muy fuerte |
| | 0-30.000€ | 30.001-90.000€ | 90.001-180.000€ | >180.000€ |

Fuente: Elaboración propia

Figura 4.4. Clasificación de los riesgos residuales en función del nivel de riesgo




Fuente: Elaboración propia

## 4.4. REVISIÓN Y MONITOREO

La efectividad de la metodología ERM depende, en gran medida, de los controles y revisiones impuestos con el propósito de evaluar el desempeño, los riesgos y los cambios significativos que hayan podido alterar las circunstancias en las que la entidad opera. A través de la monitorización de la gestión de riesgos, lo que se consigue es asegurar el correcto funcionamiento del sistema, persiguiendo así la mejora continua y la calidad de los resultados obtenidos a lo largo del tiempo. (Abella Rubio, 2006)

Para alcanzar una mejora continua se tiene que supervisar “lo que está ocurriendo” en el contexto empresarial, es decir, se deben de evaluar todos aquellos cambios tanto internos como externos que pueden afectar a los objetivos programados, y en base a dicha evaluación, se tendrá que actualizar el inventario de riesgos asociados.

En el caso concreto de la universidad que se viene analizando, la reformulación periódica del análisis DAFO constituye una posible forma para detectar las alteraciones que se vayan produciendo en el entorno. Gracias a esta herramienta, la dirección puede adaptar sus objetivos a los cambios acontecidos (ej. aparece una nueva ley que restringe la introducción de nuevas metodologías pedagógicas), a la vez que reajusta sus riesgos (ej. se reduce el impacto del riesgo asociado a la renovación de las instalaciones ante la reducción de la inflación en España) y se añade aquellos que no habían sido contemplados hasta el momento (ej. a raíz de la Covid-19, todas las organizaciones incluyeron la pandemia en su perfil de riesgos). Adicionalmente, la empresa podrá ajustar su apetito al riesgo ante el nuevo contexto observado (ej. reducción del apetito ante una posible recesión económica).

Por otra parte, también resulta necesaria la implementación de un procedimiento a través del cual se pueda revisar el grado de desempeño actual y la eficacia de las medidas implementadas. En la entidad objeto de estudio, al contar con manuales de procedimientos para todas las tareas ejecutadas, dicha revisión puede ser realizada a través de la elaboración de informes de cumplimiento. Los distintos gerentes departamentales elaboran un informe sobre el grado de cumplimiento con los procedimientos establecidos y sobre las posibles deficiencias observadas, los cuales serán posteriormente remitidos a la dirección y al órgano de gobierno para la correspondiente introducción de acciones correctivas. Esta actividad de control es fundamental ya que, además de involucrar la forma correcta de hacer las cosas, constituye un medio oportuno para que la gerencia se asegure y promueva el logro de los objetivos (Romero, 2012).

De manera adicional, serán utilizados una serie de Indicadores de Riesgo (*Key Risk Indicators*) para aspectos tales como el volumen de reservas, la cantidad de financiación externa o las tasas de rendimiento académico. A través del nivel de estas métricas se podrán identificar aquellos riesgos potenciales o emergentes donde es necesario aplicar medidas.

Finalmente, resulta relevante señalar que, de manera complementaría a los controles y revisiones ya efectuadas en la entidad analizada, se constituirá una comisión de auditoría interna paralela al consejo asesor ya existente. Esta comisión de auditoría se encargará de valorar, de forma periódica, objetiva e independiente, la idoneidad del marco de gestión adoptado y de los controles efectuados. Gracias a las valoraciones y recomendaciones aportadas por el equipo de auditoría interna se asegura la continua introducción de mejoras en el proceso de gestión de riesgos.

## 4.5. INFORMACIÓN, COMUNICACIÓN Y REPORTE

El último componente del modelo COSO-ERM es el de “Información, Comunicación y Reporte”. Todo proceso de gestión de riesgos y control interno requiere de un adecuado sistema de captación e intercambio de datos, que posibilite orientar las acciones de todos los agentes en todos los niveles de la organización hacia el mejor logro de los objetivos (Bertini et al., 2014). Para su correcto desarrollo, se deben de utilizar mecanismos y tecnologías que capturen y procesen toda la información necesaria en materia de riesgos, así como plantear políticas y directrices que aseguren la adecuada e imprescindible divulgación de la información a lo largo de toda la entidad. (Ballesteros, 2014)

Para el caso concreto de la universidad seleccionada, la información será recogida y procesada mediante un software ERM (*enterprise risk management*). Mediante la utilización de esta herramienta informática, se podrá centralizar toda la información proveniente de las distintas áreas operativas de la entidad, de tal forma que se optimice

su capacidad para anticipar, evaluar y responder adecuadamente a los riesgos. Los responsables de los distintos departamentos y áreas de la universidad contarán con acceso directo a la herramienta para la carga, análisis y reporte de los riesgos bajo su responsabilidad, y tanto el comité ejecutivo como la comisión de auditoría podrán consultar toda la información contenida en el programa para cumplir con sus responsabilidades de supervisión. Adicionalmente, se podrán utilizar otros programas de análisis de datos y big data para pronosticar y gestionar las incertidumbres y eventos de riesgo de los proyectos y del entorno.

En cuanto a la comunicación, se definirán distintos flujos y canales de aprobación y reporte, los cuales se ajustarán a las necesidades y características propias de cada nivel organizativo y área de actividad. Además, en el caso concreto del Consejo de Administración, será la comisión de auditoría la principal responsable en reportarles de manera mensual todos los datos relevantes sobre la gestión de riesgos en la empresa.

Por medio de estas corrientes de información se tendrá que transmitir una visión tanto cualitativa (tendencia histórica, perspectiva futura, nivel de aseguramiento, etc.) como cuantitativa (nivel de exposición, nivel máximo, análisis y cuantificación del impacto, etc.) de los principales riesgos y su impacto real sobre los objetivos de la sociedad (Instituto de Auditores Internos, 2021). Gracias a esta comunicación constante y a la implicación de todas las personas, desde el rango más bajo hasta el más alto, se consigue promulgar una cultura de gestión y prevención de riesgos en toda la entidad.

# 5. EVALUACIÓN SOBRE EL GRADO DE IMPLEMENTACIÓN DEL MODELO COSO-ERM.

Una vez obtenido un modelo de gestión de riesgos adaptado a las características propias de la universidad sobre la cual se han ido aplicado los 5 componentes de manera estructurada, se procede a evaluar el grado de implementación de la metodología COSO-ERM en esta institución.

Para ello, se emplea el Modelo de Madurez desarrollado por el Instituto de Auditores Internos. Esta guía incluye una serie de preguntas asociadas a cada uno de los principios del COSO-ERM, de tal manera que, una vez hayan sido todas respondidas, se obtendrá una puntuación del 1 al 5 sobre el nivel en el que la universidad ha integrado o asimilado este el modelo. Los grados de madurez contemplados para responder a las cuestiones, de menor a mayor nivel de implementación, son los siguientes (Instituto de Auditores Internos, 2021):

1. Ad hoc: El enfoque para determinar los requisitos de control interno y gestión de riesgos es ad hoc y desorganizado.
2. Fragmentada: Existen controles, pero no están documentados.
3. Global: Existen controles y están adecuadamente documentados.
4. Integrada: Existe un entorno de control interno y de gestión de riesgos efectivo.
5. Estratégica: Existe un programa integral de control interno y gestión de riesgos a nivel de empresa.

Habiendo completado el cuestionario de madurez (Anexo 8.1), se obtiene una puntuación final sobre el grado de integración del modelo COSO-ERM en la universidad creada de 4,6 sobre 5, así como el subsiguiente mapa de calor asociado, que facilita la identificación de aquellos puntos en los que aún se puede mejorar.

Cuadro 5.1. Mapa de calor sobre el grado de implementación de la metodología COSO-ERM en la universidad

| ÍNDICE GENERAL DE MADUREZ DEL SISTEMA ERM | 4,6 | Integrado | | ATENCIÓN MÁXIMA | ATENCIÓN ALTA | ATENCIÓN MEDIA | ATENCIÓN LEVE |
|---|---|---|---|---|---|---|---|
| 1. Gobierno y Cultura | 4,5 | Integrado | 35% | | | | |
| 1. Supervisión de Riesgos a través del Consejo de Adm. | 4,5 | Integrado | | | | 1. Supervisión de Riesgos a través del Consejo de Adm. | |
| 2. Establece Estructuras Operativas | 4,7 | Integrado | | | | 2. Establece Estructuras Operativas | |
| 3. Define la Cultura Deseada | 5,0 | Estratégico | | | | | 3. Define la Cultura Deseada |
| 4. Demuestra Compromiso con los Valores Clave | 4,3 | Integrado | | | | 4. Demuestra Compromiso con los Valores Clave | |
| 5. Atrae, Desarrolla, y Retiene a Profesionales Capacitados | 4,2 | Integrado | | | | 5. Atrae, Desarrolla, y Retiene a Profesionales Capacitados | |
| 2. Estrategia y Definición de Objetivos | 4,8 | Integrado | 20% | | | | |
| 6. Analiza el Contexto Empresarial | 5,0 | Estratégico | | | | | 6. Analiza el Contexto Empresarial |
| 7. Define el Apetito al Riesgo | 5,0 | Estratégico | | | | | 7. Define el Apetito al Riesgo |
| 8. Evalúa Estrategias Alternativas | 4,5 | Integrado | | | | 8. Evalúa Estrategias Alternativas | |
| 9. Formula Objetivos de Negocio | 5,0 | Estratégico | | | | | 9. Formula Objetivos de Negocio |
| 3. Desempeño | 4,8 | Integrado | 15% | | | | |
| 10. Identifica el Riesgo | 4,0 | Global | | | | | 10. Identifica el Riesgo |
| 11. Evalúa la Gravedad del Riesgo | 5,0 | Estratégico | | | | | 11. Evalúa la Gravedad del Riesgo |
| 12. Prioriza Riesgos | 5,0 | Estratégico | | | | | 12. Prioriza Riesgos |
| 13. Implementa Respuestas ante los Riesgos | 5,0 | Estratégico | | | | | 13. Implementa Respuestas ante los Riesgos |
| 4. Análisis y Revisión | 4,8 | Integrado | 15% | | | | |
| 15. Evalúa los Cambios Significativos | 4,3 | Integrado | | | | 15. Evalúa los Cambios Significativos | |
| 16. Revisa el Riesgo y el Desempeño | 5,0 | Estratégico | | | | | 16. Revisa el Riesgo y el Desempeño |
| 17. Persigue la Mejora de la Gestión del Riesgo Empresarial | 5,0 | Estratégico | | | | | 17. Persigue la Mejora de la Gestión del Riesgo Empresarial |
| 5. Información, comunicación y reporte | 4,6 | Integrado | 15% | | | | |
| 18. Aprovecha la Información y la Tecnología | 4,7 | Integrado | | | | 18. Aprovecha la Información y la Tecnología | |
| 19. Comunica Información sobre Riesgos | 5,0 | Estratégico | | | | | 19. Comunica Información sobre Riesgos |
| 20. Informa sobre el Riesgo, la Cultura y el Desempeño | 4,0 | Global | | | | | |

Fuente: Adaptado a partir del “Modelo de Madurez” del Instituto de Auditores Internos.

En síntesis, es posible destacar que gracias al adecuado desarrollo de los distintos componentes de la metodología COSO-ERM, se ha conseguido que, una sociedad que carecía de sistema de gestión de riesgos, alcance una alta implementación del mismo. No obstante, tras la valoración del mapa de riesgos obtenido (cuadro 5.1), también es necesario señalar aquellas mejoras a introducir en cada uno de los componentes:

1. Gobierno y cultura:
    a. Se debería de ofrecer una mayor formación al Consejo en materia de gestión de riesgos.
    b. Existe una clara definición de la 3º línea, pero aún es necesario delimitar las responsabilidades entre la 1º y 2º línea.
    c. Tienen que realizarse mediciones sobre el nivel de cultura de riesgos entre los empleados.
    d. No se ha desarrollado aún un plan de sucesión de los puestos clave de la gestión de riesgos.
2. Estrategia y definición de Objetivos:
    a. Se deberían emplear metodologías avanzadas para la evaluación de las estrategias alternativas tales como técnicas estadísticas, simulación Montecarlo, matrices de correlaciones, etc.
3. Desempeño.
    a. Resulta necesaria la inclusión de una taxonomía sobre todos los riesgos que se vayan identificando.
4. Revisión y Monitoreo
    a. Falta la introducción de flujos de reporte por urgencia o por excepción.

5. Información, Comunicación y Reporte:
    a. Se debe aún reportar sobre la cultura de riesgos en la entidad,
    b. Se podrían utilizar en mayor medida otras herramientas de tecnología para complementar las actividades del ERM.

# 6. CONCLUSIONES

Tras la realización del trabajo, mediante el cual ha sido expuesta la implementación desde cero de la metodología COSO-ERM de gestión de riesgos sobre una universidad privada ficticia, se extraen las siguientes conclusiones:

En primer lugar, es posible confirmar que la gestión de riesgos y el control interno, independientemente del marco de referencia utilizado, constituyen una pieza clave en la creación de valor buscada por cualquier empresa. A través de la inclusión de este sistema en el desarrollo estratégico de una organización, se consigue prevenir y afrontar los múltiples riesgos a los que está expuesta, adaptarse a los continuos cambios del entorno, facilitar la toma de decisiones y la asignación de recursos, y sobre todo mejorar la eficiencia y eficacia en torno a la consecución de los objetivos organizacionales.

En segundo lugar, se verifica que la metodología COSO es una opción muy recomendable para todas aquellas empresas interesadas en introducir un sistema de gestión de riesgos, puesto que se adapta fácilmente a las particularidades propias de cada entidad y, además, ofrece un esquema estructurado que facilita significativamente su aplicación. En este caso en concreto, se ha partido de una situación en la que no existía ningún marco de gestión de riesgos, y de manera secuencial y sencilla, se han ido desarrollando cada uno de los principios hasta la final obtención de un modelo adaptado a la entidad.

Asimismo, se ha comprobado que el modelo COSO es útil tanto para un enfoque de control o cumplimiento (ej. asegurar el cumplimiento de los requisitos legislativos a los que está sometida la universidad), o bien para alcanzar los objetivos establecidos (ej. gestionar la pérdida de control sobre el mensaje para alcanzar la efectividad del plan de comunicación).

Por último, mencionar que, a pesar de que el trabajo muestre una forma simplificada en la que es posible aplicar el modelo COSO-ERM, con la realización de los procedimientos expuestos se consigue alcanzar un grado de implementación de 4,6 sobre 5. Por ello, la metodología propuesta y desarrollada en el presente trabajo puede ser utilizada como guía a la hora de introducir este tipo de sistema de gestión de riesgos, adaptándolo siempre al modelo de negocio de cada entidad.

# 7. BIBLIOGRAFÍA

Abella Rubio, R. 2006. COSO II y la gestión integral de riesgos del negocio. *Estrategia financiera*, núm. 225, febrero. https://bit.ly/3MNeMZy

Agudelo Zapata, S.L. 2021. *La Alta Dirección y su papel en gestión de riesgos*. LinkedIn, 14 octubre. [Consulta: 15-05-2023]. https://bit.ly/41P8Bsm

Almuiñas Rivero, J.L.; Galarza López, J. 2016. Dirección estratégica y gestión de riesgos en las universidades. *Revista Cubana de Educación Superior.* vol. 35. no. 2. https://bit.ly/44wbHUt

Alvarez-Indacochea, A.A.; Pibaque-Pionce, M.S.; Moran-Chilan, J.H. 2022. Los Procesos del Control en la Gestión de Riesgo Empresarial. *Polo del Conocimiento*, Vol. 7, No 2, pp. 707-719. ISSN: 2550 - 682X. https://bit.ly/3UMgflf

Ambrosone, M. 2007. *La administración del riesgo empresarial: Una responsabilidad de todos - El enfoque COSO*. Documento de trabajo de PricewaterhouseCoopers. [Consulta: 09/05/2023]. https://bit.ly/3LTPW8J

Azcoti Navarro. 2022. *Enterprise Risk Management (ERM) como herramienta de creación de valor*. L. S. Escobar Torres (dir). Trabajo fin de grado, Universidad Pontificia de Comillas. https://bit.ly/3zPyI6G

Ballesteros, L. 2014. Información y comunicación. En: *Wordpress*, 17 mayo. [Consulta: 22-05-2023]. https://n9.cl/xijr3

Barrio Carvajal, S. 2019. Nuevas tendencias en la gestión de riesgos del control interno. *Auditoría Pública*, nº 73, pp. 43 - 51. https://bit.ly/3mIjqOq

BBVA. 2017. *Evolución de la universidad privada y resultados universitarios*. Documento de trabajo Fundación BBVA nº20/2017. [Consulta 07-05-2023]. https://bit.ly/2B7VoRZ

Bertani, E. A.; Polesello, M. F.; Sanchez, M. M.; Anibal, J. 2014. *COSO I y COSO II: una propuesta integrada*. M. A. Marín de Guerrero (dir). Trabajo de Investigación, Universidad Nacional de Cuyo. https://acortar.link/8SfMIq

Canaza Tapia, A.; Torres Aldana, L. 2018. *Gestión de riesgos empresariales COSO ERM 2017 y la prevención de fraude en las empresas del sector industrial que cotizan en la Bolsa de Valores de Lima*. E. Lau Rebolledo (dir). Tesis, Universidad Peruana de Ciencias Aplicadas. https://bit.ly/3I3hSWP

Carbante, J.M. 2023. Universidades en España: las privadas recortan distancias. *ACEprensa*, 30 enero. [Consulta: 07-05-2023]. https://bit.ly/3plZXEa

Castro, J. 2022. ¿Qué es el Control Interno de una empresa?. En: *Blog Corponet*, 15 julio. [Consulta: 19-03-2023]. https://bit.ly/3mi2oXj

Cobb, M. 2021. ISO 31000 vs. COSO: Comparing risk management standards. En: *Techtarget Network* [blog], 12 octubre. [Consulta: 23-03-2023]. https://bit.ly/3MxvKLS

Conejos Merita, P. 2018. *Marco de apetito y tolerancia al riesgo. Integración en la gestión.* I. Oñate Rodríguez de Borbolla (dir). Trabajo fin de máster, Universidad Pontificia de Comillas. https://bit.ly/42mIf23

Deloitte. 2020. *Apetito al riesgo. Ajustando los riesgos a nuestra medida.* Boletín de Gobierno Corporativo de Deloitte. [Consulta: 08-05-2023]. https://bit.ly/3I1gFPF

Díaz Barriga, F. 2005. *Enseñanza situada: Vínculo entre la escuela y la vida*. México, MX: McGraw Hill. ISBN: 970-10-5516-0. https://bit.ly/3LNBDlV

Equipo Orca. 2022. Recomendaciones para el éxito en la gestión de riesgos y control interno. En: *Orca organizational risk and compliance administration* [Blog], 11 enero. [Consulta: 19-03-2023]. https://bit.ly/3GWwKWr

Hasper Tabares, J.; Correa Jaramillo, J.; Benjumea Arias, M.; Valencia Arias, A. 2017. Tendencias en la investigación sobre gestión del riesgo empresarial: un análisis bibliométrico. *Revista Venezolana de Gerencia*, vol. 22, núm. 79, pp. 507. ISSN: 1315-9984. https://bit.ly/3pP4X4v

Global Institute of Internal Auditors. 2020. *El modelo de las tres líneas del IIA 2020. Una actualización de las tres líneas de defensa.* Fundación latinoamericana de auditores internos. [Consulta: 21-03-2023]. https://bit.ly/3A5yFUq

Instituto de Auditores Internos de España. 2021. *Auditoría Interna y gestión de riesgos.* En: La fábrica del pensamiento. [Consulta: 18-03-2023]. https://bit.ly/3p4tCRX

Instituto de Auditores Internos de España. 2013. *Definición e implantación de apetito de riesgo.* En: La fábrica del pensamiento. [Consulta: 09-05-2023]. https://bit.ly/3LKUG0o

Instituto Nacional de Estadística y Geografía. 2014. Cuestionario de autoevaluación del control interno. [Consulta 28-04-2023]. https://bit.ly/42sanR0

International Organization for Standarization. 2018. ISO 31000. *Gestión del riesgo — Directrices*. [Consulta: 22-03-2023]. https://bit.ly/3ooQ33T

Martinez, F. L. 2019. *Nuevo modelo de gestión de riesgos en las organizaciones (Tres Líneas de Defensa).* D.E. León Lopez (dir.) Trabajo de grado, Universidad Militar de Nueva Granada. http://hdl.handle.net/10654/32624.

Martínez Torre-Enciso M.I.; Casares San José-Martí M.I. 2011. El proceso de gestión de riesgos como componente integral de la gestión empresarial. *Boletín de Estudios económicos de la Universidad Comercial de Deusto*, vol. LXVI, no. 202, pp. 73-94. https://bit.ly/3InTlvs

OCDE. 2018. Estudio de la OCDE sobre Integridad en el Estado de Nuevo León, México: Dando sostenibilidad a las reformas de integridad. *Estudios de la OCDE sobre Gobernanza Pública, Éditions OCDE, Paris*, pp. 192-203. https://bit.ly/3Mvi6st

Oracle. 2023. Aplicaciones. ERP. Gestión de riesgos y cumplimiento. ¿Qué es Enterprise Risk Management (ERM)?. [Consulta: 19-03-2023]. https://bit.ly/3GR1F6i

Ortega, A. 2022. Automatización del modelo de las 3 líneas de defensa. En: *GlobalSuite Solutions*, 12 agosto. [Consulta 20-03-2023]. https://bit.ly/3KpWqeG

Perez, A. 2018. Conoces los pasos para elaborar el plan de comunicación de una empresa. En: *OBS Business School* [blog], 28 febrero. [Consulta: 07-05-2023]. https://bit.ly/42zx8SW

Price Waterhouse Coopers. 2017. *Gestión del Riesgo Empresarial. Integrando Estrategia y Desempeño.* Documento de trabajo del Committee of Sponsoring Organizations of the Treadway Commission. [Consulta: 24-03-2023]. https://bit.ly/2nSCk6q

Pursell, S. 2023. ¿Qué son los objetivos operativos y por qué establecerlos? En: *Hubspot* [blog], 9 marzo. [Consulta: 06-05-2023]. https://bit.ly/3BaNztj

Risk and Insurance Management Society. 2011. *An Overview of Widely Used Risk Management Standards and Guidelines.* Joint Report of RIMS Standards and Practices Committee and RIMS ERM Committee. [Consulta: 22-03-2023]. https://bit.ly/3mFw7tj

Roa, M.; Mejía, G.; Rubio, C. 2017. *COSO ERM 2017 y la Generación de Valor*. Deloitte. [Consulta: 20-03-2023]. https://bit.ly/3p4uB4B

Romero, J. 2012. Control interno y sus 5 componentes según COSO. En: *Gestiopolis* [Blog], 31 agosto. [Consulta: 18-05-2023]. https://bit.ly/2RMWM2s

Seguridad Minera. 2020. Norma ISO 31000:2018: principios y marco de referencia para la gestión de riesgos. En: *Revista Seguridad Minera*, 27 noviembre. [Consulta: 22-03-2023]. https://bit.ly/3KPEAmU

Silva Quiroz, J.; Maturana Castillo, D. 2017. Una propuesta de modelo para introducir metodologías activas en educación superior. *Revista de Innovación Educativa (Méx. DF)* vol.17 no.73. ISSN 1665-2673. https://bit.ly/3LI0sQt

Society of Corporate Compliance and Ethics & Health Care Compliance Association. 2020. *Compliance risk management: Applying the COSO ERM framework*. Documento de trabajo de Committee of Sponsoring Organizations of the Treadway Commission. [Consulta: 30-04-2023]. https://bit.ly/41exxJC

Steph, C. 2016. El análisis DAFO: *Los secretos para fortalecer su negocio (Gestión y Marketing).* 50 Minutos.es (ed). ISBN: 2806285771. https://bit.ly/3HHLCIi

Terreros, D. 2023. Control interno empresarial: sus elementos, objetivos e importancia. En: *Hubspot* [blog], 1 marzo. [Consulta: 19-03-2023]. https://bit.ly/3UrcDVG

Tien Can, D. 2021. Corporate Governance; Update of the three lines of defense model. En: *Ordre de comptables pròfessionnels agréés du Québec*, 16 abril. [Consulta 20-03-2023]. https://bit.ly/3ZThbW6

Tur-Viñes, V.; Monserrat-Gauchi, J. 2014. El plan estratégico de comunicación. Estructura y funciones. *Razón y Palabra (Ecuador)*. No 88. ISSN: 1605-4806. https://bit.ly/3M8Rc9m

Westreicher, G. 2021. *Riesgo empresarial*. Economipedia. [Consulta:15-05-2023]. https://bit.ly/3IlLxdG

# 8. ANEXOS

Anexo 8.1. Cuestionario de Madurez de la universidad creada.

| Componente | Principio | Puntos de Reflexión | Grado de Madurez |
|---|---|---|---|
| 1. Gobierno y Cultura | 1. Supervisión de Riesgos a través del Consejo de Adm. | 1.1. El Reglamento del Consejo establece sus competencias en materia de supervisión de gestión de riesgos? | 5.- Estratégico |
| | | 1.2. Los miembros del Consejo de Administración reciben formación personalizada para cumplir con sus deberes de supervisión de la gestión de riesgos? | 3.- Global |
| | | 1.3. Existe una Política de Gestión de Riesgos, aprobada por el Consejo de Administración, donde se establecen los principales roles, responsabilidades y competencias? | 5.- Estratégico |
| | | 1.4. La política de gestión de riesgos es consistente con otros marcos relacionados (v.g.; seguridad, calidad, cumplimiento, etc.) ? | 5.- Estratégico |
| | 2. Establece Estructuras Operativas | 2.1. La compañía ha articulado un marco formal de gestión de riesgos | 5.- Estratégico |
| | | 1.4. El marco es consistente con otros marcos relacionados (v.g.; seguridad, calidad, cumplimiento, etc.) ? | 5.- Estratégico |
| | | 2.2. El marco de gestión de riesgos ha sido ampliamente comunicado a través de la organización | 5.- Estratégico |
| | | 2.3. Están claramente establecidos los flujos de aprobación y reporte en la gestión de riesgos? | 5.- Estratégico |
| | | 2.4. Existe una función de gestión de riesgos independiente de la dirección? | 5.- Estratégico |
| | | 2.5. Están claramente identificados los agentes de 1a., 2a y 3a Línea de Defensa en las principales áreas de la organización? | 3.- Global |
| | | 2.6. Existe un Comité de Riesgos o se tratan dichos asuntos en alguno de los Comités existentes? | 5.- Estratégico |
| | | 2.7. Los responsables de riesgos de las áreas/líneas de negocio (p.ej. Seguridad, Cliente, RRHH, Legal, etc.) comparecen periódicamente en dicho Comité? | 5.- Estratégico |
| | 3. Define la Cultura Deseada | 3.1. Existe un Código ético? | 5.- Estratégico |
| | | 3.2. La organización personaliza su marco de gestión de riesgos basado en su cultura? | 5.- Estratégico |
| | | 3.3. La Política de Riesgos refleja los principios de comportamiento esperado, conforme a lo previsto en el Código Ético de la organización? | 5.- Estratégico |
| | 4. Demuestra Compromiso con los Valores Clave | 4.1. Se ponen a disposición del conocimiento público, tanto interno como externo, los principales valores de la organización? | 5.- Estratégico |
| | | 4.2. Demuestra la Alta Dirección con su comportamiento su compromiso con los valores de la organización (tone at the top)? | 5.- Estratégico |
| | | 4.3. Demuestra la Alta Dirección con su comportamiento su compromiso con ERM (tone at the top)? | 5.- Estratégico |
| | | 4.4. Los miembros del Comité de Riesgos promueven activamente la cultura de gestión de riesgos entre el personal de sus áreas de responsabilidad? | 5.- Estratégico |
| | | 4.5. El proceso de inducción de nuevos empleados incorpora un módulo de culturización sobre riesgos? | 5.- Estratégico |
| | | 4.6. Se realizan mediciones / evaluaciones sobre el nivel de cultura de riesgos entre los empleados de forma regular? | 1.- Ad-Hoc |
| | 5. Atrae, Desarrolla, y Retiene a Profesionales Capacitados | 5.1. Existe un programa de gestión del talento? | 5.- Estratégico |
| | | 5.2. Existe una política de la compañía, soportando su compromiso con el desarrollo de los empleados, un sistema de compensación justo, la diversidad y el respeto de los derechos humanos? | 5.- Estratégico |
| | | 5.3. El personal de gestión de riesgos dispone de las habilidades y conocimiento necesario para realizar sus tareas | 5.- Estratégico |
| | | 5.4. Los objetivos del personal de gestión de riesgos están alineados con los de la función ERM | 5.- Estratégico |
| | | 5.5. Existe un plan de sucesión para los puestos clave de gestión de riesgos? | 1.- Ad-Hoc |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez |
|---|---|---|---|
| 2. Estrategia y Definición de Objetivos | 6. Analiza el Contexto Empresarial | 6.1. Existe un Plan estratégico aprobado por el Consejo de Administración? | 5.- Estratégico |
| | | 6.2. El registro/inventario de riesgos refleja los factores internos y externos que puedan repercutir sobre los objetivos de la organización (estratégicos, de operaciones, etc.)? | 5.- Estratégico |
| | | 6.3. Se analiza de forma sistemática la información externa para identificar los cambios relevantes en el contexto de negocio e identificar riesgos emergentes? | 5.- Estratégico |
| | | 6.4. Se analiza de forma sistemática la información interna para identificar los cambios relevantes en el contexto de negocio e identificar riesgos emergentes? | 5.- Estratégico |
| | 7. Define el Apetito al Riesgo | 7.1. Existe una "declaración del apetito al riesgo" adecuadamente formalizada? | 5.- Estratégico |
| | | 7.2. Es competencia exclusiva del Consejo de Administración la definición del apetito al riesgo? | 5.- Estratégico |
| | | 7.3. Se promueve activamente que la Alta Dirección y los agentes clave ERM conozcan el apetito al riesgo de la organización? | 5.- Estratégico |
| | | 7.4. El apetito al riesgo es considerado en los procesos de toma de decisiones? | 5.- Estratégico |
| | | 7.5. Se involucra al Consejo de Administración en la toma de decisiones que pudieran implicar incumplir con el apetito al riesgo establecido? | 5.- Estratégico |
| | | 7.6. Se monitoriza activamente el cumplimiento con el apetito al riesgo? | 5.- Estratégico |
| | 8. Evalúa Estrategias Alternativas | 8.1. La estrategia de la compañía está alineada con su misión, visión y valores? | 5.- Estratégico |
| | | 8.2. En el proceso de planificación estratégica, se evalúan estrategias alternativas, analizándose los riesgos y oportunidades asociados basándose en metodologías probadas (v.g.; técnicas estadísticas, simulación Montecarlo, matrices de correlaciones, etc.)? | 4.- Integrado |
| | | 8.3. Participan sistemáticamente los agentes clave ERM en el proceso de planificación estratégica? | 5.- Estratégico |
| | 9. Formula Objetivos de Negocio | 9.1. Los objetivos estratégicos de la organización están alineados con el apetito al riesgo establecido? | 5.- Estratégico |
| | | 9.2. Los objetivos estratégicos son desarrollados en objetivos de operaciones, financieros, cumplimiento, etc.? | 5.- Estratégico |
| | | 9.3. Están los objetivos de los empleados alineados a los objetivos estratégicos de la organización? | 5.- Estratégico |
| | | 9.4. Se definen y actualizan los niveles de tolerancia al riesgo para todos los riesgos clave con la aprobación del Consejo de Administración? | 5.- Estratégico |
| | | 9.5. Los niveles de tolerancia al riesgo son considerados en los procesos de toma de decisiones? | 5.- Estratégico |
| | | 9.6. Se monitoriza activamente el cumplimiento con los niveles de tolerancia al riesgo? | 5.- Estratégico |
| | | 9.7. Las excepciones al cumplimiento con la tolerancia al riesgo son gestionadas caso a caso y requieren aprobación de la Alta Dirección y/o el Consejo de Administración? | 5.- Estratégico |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez |
|---|---|---|---|
| 3. Desempeño | 10. Identifica el Riesgo | 10.1. Existen procesos para identificar sistemáticamente los principales riesgos y oportunidades que repercuten en la consecución de los objetivos estratégicos y de negocio? | 5.- Estratégico |
| | | 10.2. Se identifican y evalúan los riesgos periódicamente, al menos con carácter anual? | 5.- Estratégico |
| | | 10.3. Existe una taxonomía de riesgos para catalogar los riesgos por tipología? | 1.- Ad-Hoc |
| | | 10.3. Se definen KRIs (*Key Risk Indicators)* para identificar proactivamente riesgos con crecientes o emergentes? | 5.- Estratégico |
| | 11. Evalúa la Gravedad del Riesgo | 11.1. Se evalúa el impacto y probabilidad de los riesgos identificados con criterios homogéneos prestablecidos? | 5.- Estratégico |
| | | 11.2. Se cuantifica el impacto económico de los riesgos, siempre que sea posible? | 5.- Estratégico |
| | | 11.3. Se considera el impacto reputacional de los riesgos? | 5.- Estratégico |
| | 12. Prioriza Riesgos | 12.1. Los riesgos se priorizan en base a su impacto y probabilidad de ocurrencia? | 5.- Estratégico |
| | | 12.2. Los riesgos se representan en un mapa de riesgos (v.g.; mapa de calor) que habilita su priorización? | 5.- Estratégico |
| | | 12.3. Se monitoriza sistemáticamente que la severidad de los riesgos cumple con el apetito / tolerancia al riesgo establecidos? | 5.- Estratégico |
| | 13. Implementa Respuestas ante los Riesgos | 13.1. Se definen planes para gestionar todos los riesgos identificados (i.e.; aceptar, evitar, mitigar, o transferir)? | 5.- Estratégico |
| | | 13.2. Se asigna un responsable y fecha de ejecución para gestionar cada uno de los riesgos identificados? | 5.- Estratégico |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez |
|---|---|---|---|
| 4. Análisis y Revisión | 15. Evalúa los Cambios Significativos | 15.1. Existe un proceso de monitorización para identificar periódicamente los cambios del contexto empresarial (i.e.; los factores internos y externos) con posible impacto en la consecución de los objetivos de la organización? | 5.- Estratégico |
| | | 15.2. Se actualiza periódicamente el registro/inventario de riesgos de la organización, incorporando temas emergentes o cambios en el contexto de negocio? | 5.- Estratégico |
| | | 15.3. El Comité de Riesgos se reúne periódicamente para analizar, concluir y actualizar el Perfil de Riesgos de la organización? | 5.- Estratégico |
| | | 15.4. Se dispone de un proceso de reporte de urgencia o por excepción (i.e.; fuera del calendario de reporte formalmente establecido)? | 2.- Fragmentado |
| | 16. Revisa el Riesgo y el Desempeño | 16.1. La organización realiza un seguimiento periódico del grado de desempeño para los principales objetivos establecidos | 5.- Estratégico |
| | 17. Persigue la Mejora de la Gestión del Riesgo Empresarial | 17.1. La organización revisa la idoneidad y actualiza su marco de gestión de riesgos periódicamente (v.g.; auditorías)? | 5.- Estratégico |
| | | 17.2. Se han implantado mejoras significativas en el proceso de gestión de riesgos en el último año? | 5.- Estratégico |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez |
|---|---|---|---|
| 5. Información, comunicación y reporte | 18. Aprovecha la Información y la Tecnología | 18.1. Los miembros del Comité de Riesgos tienen acceso directo a la Información de riesgos que necesitan para cumplir con sus responsabilidades de supervisión | 5.- Estratégico |
| | | 18.2. Se dispone de una herramienta informática de ERM? | 5.- Estratégico |
| | | 18.3. Los agentes de 1a. Y 2a. Línea de Defensa tienen acceso directo a la herramienta para la carga, análisis y reporting de los riesgos bajo su responsabilidad? | 5.- Estratégico |
| | | 18.4. Se hace uso de herramientas de tecnología de punta (v.g.; data analytics, big data, inteligencia artificial) para complementar las actividades de ERM? | 4.- Integrado |
| | 19. Comunica Información sobre Riesgos | 19.1. Están claramente establecidos los flujos de aprobación y reporte de la información en materia de riesgos? | 5.- Estratégico |
| | | 19.2. Se reportan periódicamente (al menos de forma anual) los principales riesgos de la organización al Consejo de Administración vía la Comisión de Auditoría? | 5.- Estratégico |
| | 20. Informa sobre el Riesgo, la Cultura y el Desempeño | 20.1. Existen procesos de reporting customizado a los diferentes niveles organizativos? | 5.- Estratégico |
| | | 20.3. Se utilizan métricas de monitorización del riesgo (Key Risk Indicators o KRIs) para alertar respecto de riesgos crecientes o emergentes ? | 4.- Integrado |
| | | 20.4. Se reporta una visión tanto cualitativa (tendencia histórica, perspectiva futura, nivel de aseguramiento, etc.) como cuantitativa (nivel de exposición, nivel máximo, análisis de sensibilidad y test de estrés, etc.) de los principales riesgos? | 5.- Estratégico |
| | | 20.7. Se reportan los riesgos materializados y su impacto real sobre los objetivos de la organización? | 5.- Estratégico |
| | | 20.8. Se reporta sobre la cultura de riesgos? | 1.- Ad-Hoc |

Fuente: Adaptado a partir del “Modelo de Madurez” del Instituto de Auditores Internos.