Marcos y estándares GRC

El uso de marcos de referencia y estándares permite impulsar programas de Gobierno, Riesgo y Cumplimiento apropiados para cada organización. A continuación, se presentan algunos de los principales relacionados con este programa que se pueden adoptar de manera integral en las organizaciones:

COBIT

Control Objectives for Information and Related Technologies (ISACA, 2019) es un marco de referencia para el gobierno y la gestión de la información y la tecnología empresarial, dirigido a toda la empresa.

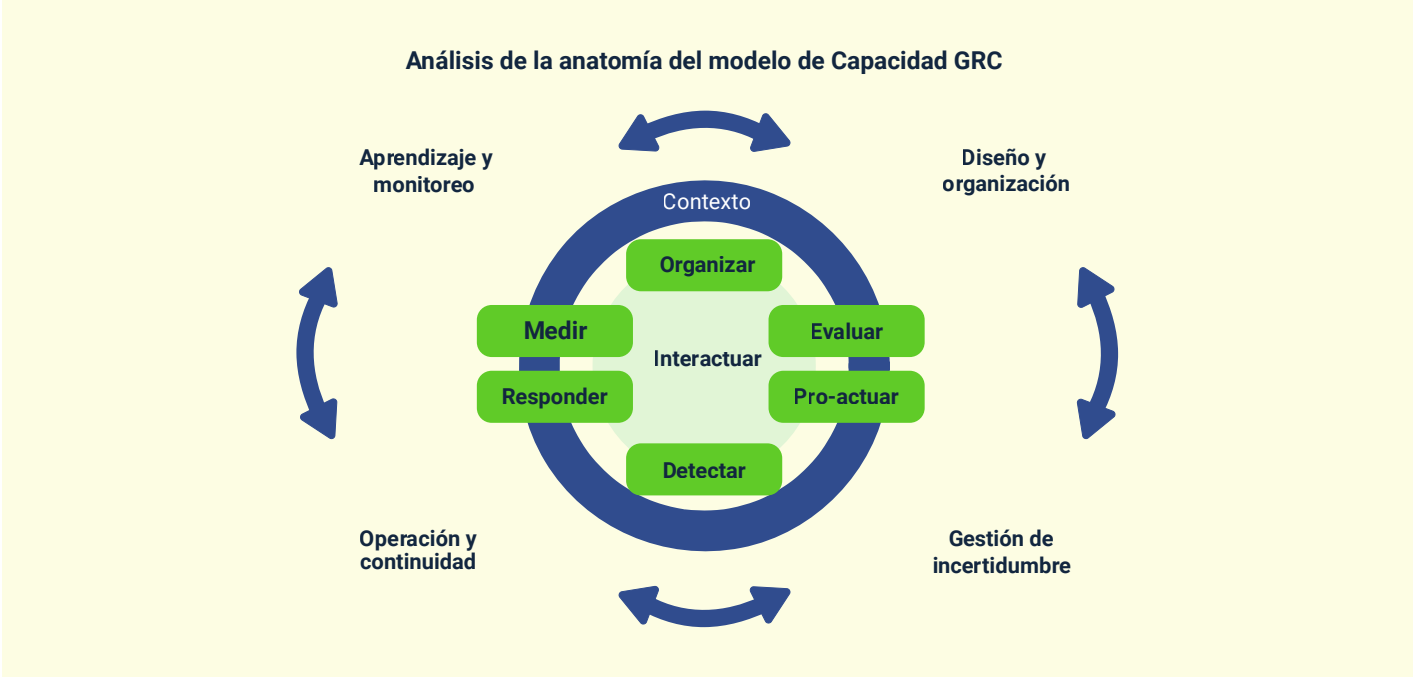
Integra varios estándares para procesos específicos, como COSO, para controles internos; ITIL, para alinearse con las necesidades de la empresa; BiSL, enfocada en la demanda de información; el estándar ISO 27000, de seguridad para TI; el entrenamiento en mejoras de procesos, CMMI; TOGAF, para la arquitectura empresarial; y PMBOK, para manejo de proyectos.

Modelo de capacidad GRC -OCEG

Este modelo de capacidad de GRC es el primer y único estándar de código abierto que integra las diversas subdisciplinas de gobierno, riesgo, auditoría, cumplimiento, ética/cultura y TI en un enfoque unificado basado en principios (OCEG, 2022).

Este estándar se puede usar para abordar una variedad de situaciones y áreas temáticas, desde anticorrupción hasta continuidad comercial y administración de terceros. El modelo es una excelente herramienta para enmarcar conversaciones sobre las capacidades de GRC con la junta directiva, los altos ejecutivos y los gerentes.

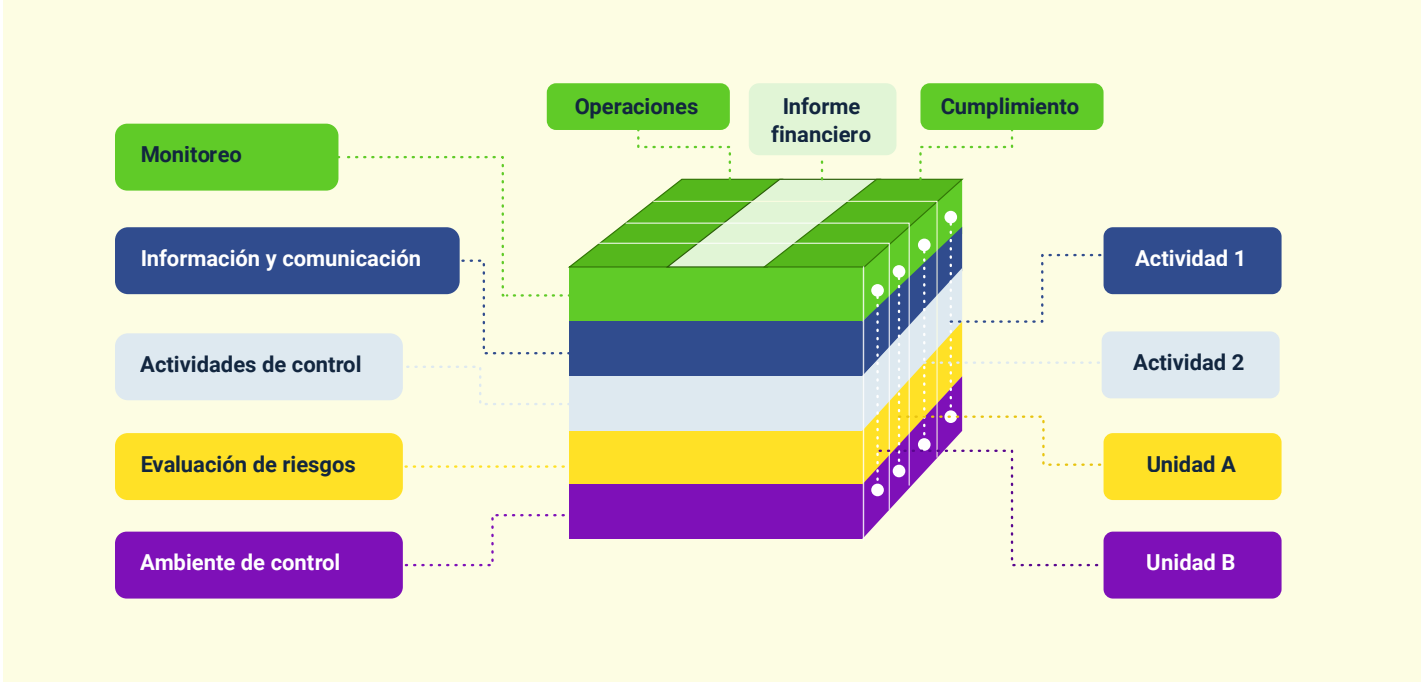
Figura 1. *Modelo de capacidad GRC*



Modelo COSO

Para gestión de riesgos. Sus siglas responden a *Committee of Sponsoring Organizations of the Treadway*, que es una organización de carácter voluntario constituida por representantes de cinco organizaciones del sector privado en Estados Unidos. Nace en 1985 con la misión de crear y proporcionar conocimiento frente a la gestión del riesgo empresarial (ERM), el control interno y la lucha contra el fraude.

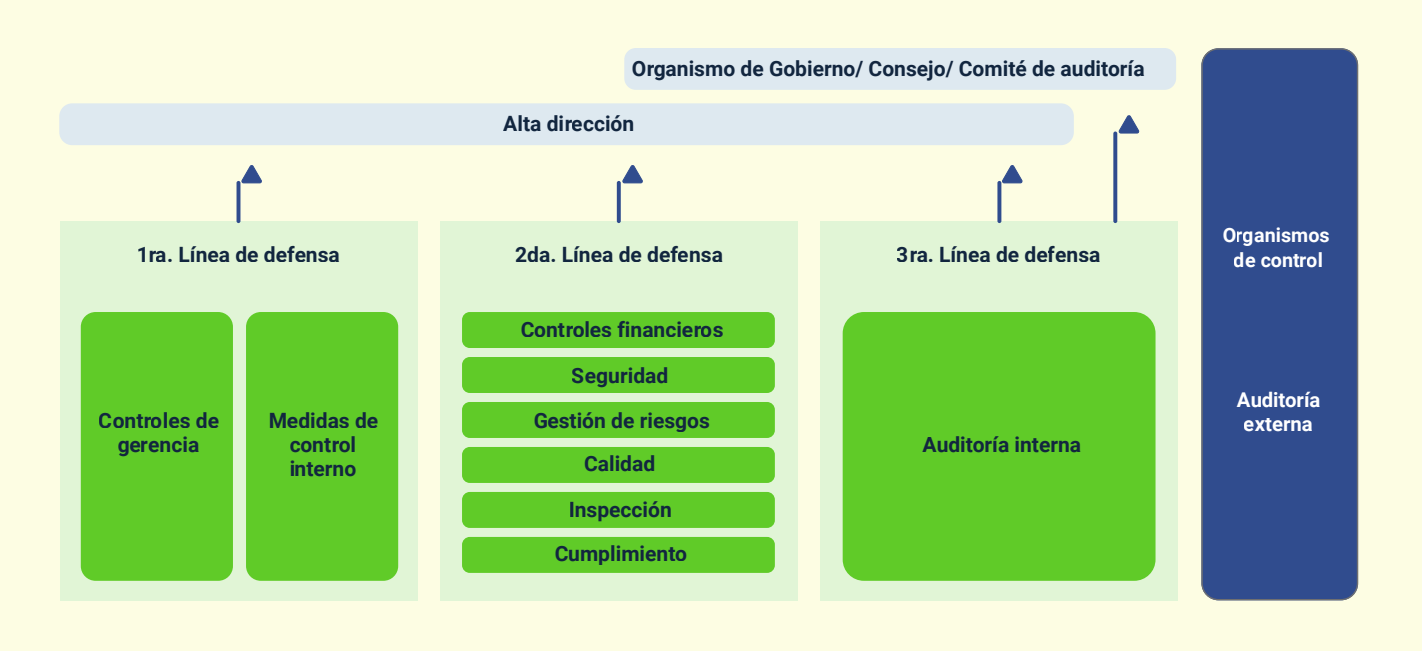
Figura 2. *Modelo COSO*



Modelo de las tres líneas

Promueve un gobierno sólido y la gestión de riesgo. El IIA Instituto de Auditores Internos, en el año 2020, actualizó el modelo de gestión de riesgo y control, "Modelo de las tres líneas de defensa", por un modelo de interconexión de los roles: Órgano de Gobierno, Gerencia y Auditoría Interna, para asegurar las condiciones de cumplimiento de la organización.

Figura 3. *Modelo de las tres líneas*



La norma ISO 31000:2018

Contiene los principios y guías para la gestión de riesgo, y define el riesgo, no de la manera tradicional, enfocado en las posibles pérdidas, sino como el efecto de la incertidumbre en los objetivos de la empresa (ISO, 2018). La ISO 31000:2018, aunque no es certificable, permite a las organizaciones de todos los sectores, sin importar que sean públicas o privadas, incorporar estándares y procesos de alto nivel para evaluar y mitigar cualquier tipo de riesgo en todas sus operaciones.

ISO 37301:2021

Compliance Management System se crea como respuesta al creciente interés de las empresas por alinear sus sistemas de gestión de cumplimiento de acuerdo con normas internacionales. Esta reemplazó a la ISO 19600:2014 *Compliance Management Systems – Guidelines.* El documento especifica los requisitos y proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión del *"compliance"* eficaz dentro de una organización. El documento es aplicable a toda clase de organizaciones, independientemente del tipo, tamaño y naturaleza de la actividad, así como a organizaciones del sector público, privado o sin fines de lucro.