Gestión Integral de Riesgos

Federico García

Socio – Risk Advisory Consulting

KPMG Costa Rica

Jornada 2022

KPMG

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Agenda:

Jornada 2022

1. Conceptos de Riesgos
2. Etapas de la Gestión Integral de Riesgos
3. Generalidades de los Riesgos Financieros
4. Generalidades de los Riesgos No Financieros
5. Generalidades del Riesgo de Fraude
6. Generalidades del Riesgo de *Compliance*

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

¿Qué entendemos por riesgo?

Jornada 2022

Se refiere a la incertidumbre existente en el logro de los objetivos, originada por eventos adversos, los cuales repercuten en el cumplimiento de los objetivos estratégicos.

Riesgos No Financieros

Es la posibilidad de pérdidas económicas producidas por la materialización de los siguientes riesgos:

- Riesgo Operativo
- Riesgo Legal
- Riesgo Reputacional
- Riesgo de Tecnologías de Información
- Riesgo de Fraude
- Riesgo de Cumplimiento

Riesgos Emergentes

- Cambios demográficos
- Cambios tecnológicos
- Gustos y preferencias de los consumidores

Riesgos Financieros

Es la posibilidad de pérdidas económicas producidas por la materialización de los siguientes riesgos:

- Riesgo de Crédito
- Riesgo de Mercado (tasas de interés, tipo de cambio y precio)
- Riesgo de liquidez

KPMG

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Etapas de la Gestión Integral de Riesgos (financieros y no financieros)

Jornada 2022

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Jornada 2022

Generalidades de los Riesgos Financieros

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

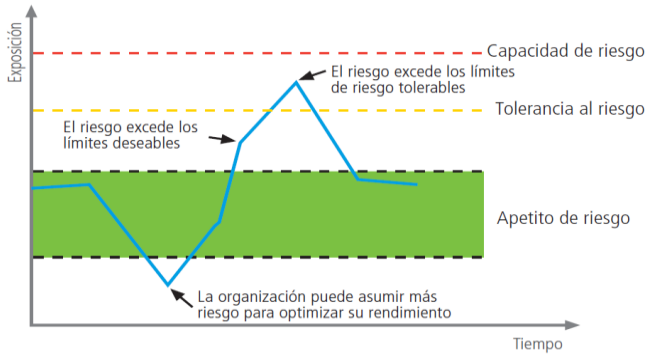
Generalidades de los Riesgos Financieros

Jornada 2022

Indicadores clave de riesgo o KRI (*Key Risk Indicators*)

Los riesgos financieros por lo general son gestionados mediante los KRI's.

- ✓ Ayudan a establecer niveles de alerta / límites para la toma de acciones por parte de las áreas involucradas.
- ✓ Cuando son diseñados y utilizados correctamente, las métricas de riesgos tienen un valor predictivo y pueden actuar como alertas tempranas para permitir acciones anticipadas.



Apetito al riesgo

Se refiere al nivel y los tipos de riesgo que la entidad está dispuesta a asumir, para lograr sus objetivos estratégicos y su plan de negocio. Este apetito debe ser aprobado por la Junta Directiva/Órgano de Dirección.

Otros conceptos a tomar encuenta:

- ✓ **Tolerancia al riesgo:** cantidad de riesgo que la entidad está dispuesta a aceptar para lograr sus objetivos.
- ✓ **Capacidad máxima de riesgo:** límite de riesgo máximo que, de ser asumido por la entidad, la expone a importantes compromisos en su patrimonio, incumplimientos de la normativa aplicable y perjuicios en su reputación corporativa.

Manejo de excepciones a los límites de riesgo

En caso de materializarse desviaciones sobre los límites de riesgo:

- ✓ Se debe informar sobre la desviación de forma inmediata al área correspondiente, a la Gerencia General y al Comité de Riesgos.
- ✓ El área dueña del riesgo y responsable de su control debe suministrar información sobre las causas de los excesos a los límites de tolerancia y se deberá identificar las posibles consecuencias.
- ✓ La Administración deberá formular **medidas correctivas** para llevar el indicador dentro de los parámetros establecidos.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Generalidades de los Riesgos Financieros

Jornada 2022

Plan de Contingencia de Liquidez

Deberá considerar medidas técnicas, humanas y organizativas para garantizar la continuidad del negocio y sus operaciones, permitiéndole a la entidad hacer frente a situaciones de iliquidez propias, u originadas por eventos imprevistos.

Este Plan debe ayudar a que la Junta Directiva/Órgano de Dirección, la Administración y el personal clave estén preparados para responder a situaciones de estrés.

Aspectos a considerar en el Plan de Liquidez:

- ✓ Señales de alerta
- ✓ Equipo de gestión de crisis
- ✓ Identificación de fuentes de financiamiento
- ✓ Estrategias de gestión de activos y pasivos
- ✓ Identificación de activos que sirvan de garantía para obtener financiamiento
- ✓ Políticas y procedimientos administrativos

Plan de Contingencia de Mercado

Debe establecer claramente la estrategia para afrontar situaciones de emergencia frente al riesgo de mercado, riesgo de tasas de interés y riesgo de tipos de cambio.

- El Plan debe ser proporcional a la dimensión de la entidad, su perfil de riesgo y a la naturaleza y complejidad de sus operaciones.
- El Plan debe ser revisado y sometido a prueba en forma regular para asegurar su eficacia y viabilidad y estar diseñado para afrontar los escenarios planteados por la entidad en las pruebas de tensión.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Jornada 2022

Generalidades de los Riesgos No Financieros

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

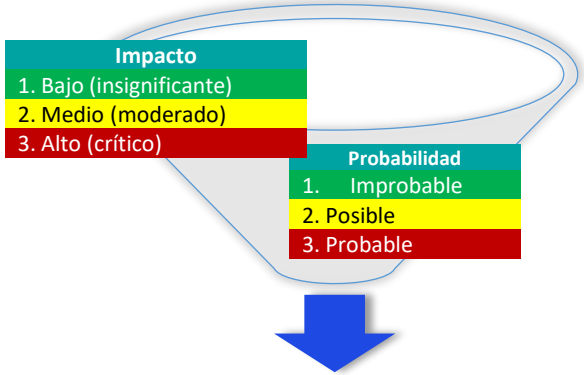
Generalidades de los Riesgos No Financieros

Jornada 2022

Riesgo inherente

Intrínseco a las actividades, procesos o sistemas, al que se enfrenta la entidad en ausencia de acciones o controles tendientes a modificar la probabilidad o impacto del riesgo.

Riesgo inherente =
Probabilidad de ocurrencia • Impacto



Resultado de la *Probabilidad de ocurrencia * Impacto*	Criticidad de riesgo
Igual o mayor a 6	Alto
Igual o mayor a 3 y menor a 6	Moderado
Igual o mayor a 1 y menor a 3	Bajo

Evaluación de controles

Los controles son evaluados para mitigar los riesgos. Diseñados con el propósito de proporcionar un grado de seguridad razonable para el logro de los objetivos.

DISEÑO	EFECTIVIDAD
Correlación	Implementación
Segregación de funciones	Documentación soporte
Competencias	Oportunidad
Frecuencia del control	Aprobación
Madurez	Respuesta

Podrían operar pero no están bien diseñados.

Podrían estar bien diseñados pero no operan de forma correcta.

Riesgo residual

Evaluación del riesgo identificado, considerando la evaluación del control y del resultado sobre su efectividad, tendientes a modificar la probabilidad o el impacto del mismo.

Riesgo residual =
Probabilidad de ocurrencia • Impacto

- ✓ Solo si, el diseño del control es adecuado, se procede a evaluar su efectividad.
- ✓ Se debe definir el responsable de evaluar el funcionamiento de los controles
- ✓ Realizar evaluaciones periódicas de la suficiencia de los controles.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Generalidades de los Riesgos No Financieros

Jornada 2022

Plan de Continuidad de negocio

Permite mantener la operativa de forma razonable ante la ocurrencia de eventos externos, errores humanos y deficiencias o fallas en los procesos que pueden crear interrupciones o inestabilidad en las operaciones de la entidad.

- ✓ Se deben mantener esquemas de comunicación y monitoreo para la identificación de incidentes.
- ✓ Activar las medidas contingentes y el proceso de recuperación. La activación de planes de continuidad facilita el mantenerse en niveles aceptables de operación.
- ✓ La gestión de incidentes hace que las unidades técnicas incorporen una labor de monitoreo, escalamiento y seguimiento sobre cada incidente.
- ✓ Comunicación de incidentes a las partes interesadas.
- ✓ Dependiendo de la gravedad de la crisis, se valora la activación la Comisión de Crisis de Continuidad del Negocio.

Plan de comunicación de crisis

Debe proporcionar una guía de las actividades de respuesta y planes de contingencia ante la materialización de un incidente crítico que pueda afectar, de forma negativa, la imagen y la reputación de la entidad.

Administración de comunicaciones internas y externas: En toda crisis debe existir un proceso formal y probado de comunicación, el cual debe ser puesto en operación cada vez que se presenten situaciones de este tipo.

Valoración post crisis: Una vez superada la crisis y realizado el proceso de vuelta a la normalidad, se debe realizar una **valoración de los puntos únicos de falla**, **oportunidades de mejora y lecciones aprendidas**, que permitan examinar a detalle lo sucedido y determinar las acciones correctivas inmediatas, mismas que deberán ser comunicadas a las partes interesadas.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Bases de datos

Jornada 2022

Incidencias

Sucesos que, siendo cuantificables, hayan generado pérdidas para la entidad por la materialización de un riesgo operativo.

Eventos potenciales

Sucesos que podrían derivar en pérdidas económicas.

Eventos externos

Sucesos que podrían derivar en pérdidas económicas, asociados a agentes externos a la entidad como clientes, proveedores, entre otros.

La base de datos de incidencias y eventos de riesgo, permite:

- Establecer de forma cuantitativa la exposición al riesgo operativo de la entidad.
- Suministrar información sobre cuáles son los eventos más relevantes.
- Permite mantener actualizadas las valoraciones de los riesgos potenciales identificados en los mapas de riesgo.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Tercerización

Jornada 2022

Selección y contratación de proveedores

Políticas, procedimientos y controles necesarios para:

- Conducir el proceso de selección.
- Monitorear los procesos o servicios subcontratados.

Clasificación de proveedores según su criticidad.

Definición formal, continuidad y seguridad

- Criterios para calificación y selección.
- Contratación:
  - Legalidad y formalidad de contratos
  - Acuerdos del nivel de servicio y cláusulas sobre continuidad y seguridad de la información.
- Responsabilidad del proveedor y la entidad.
- Pruebas a los planes de continuidad y seguridad.
- Gestión de riesgos de tercerización

Debida diligencia

La entidad aplica la diligencia debida al seleccionar posibles proveedores de servicios.

Controles a los servicios de TI tercerizados

La entidad debe considerar los controles aplicables a los servicios de TI suministrados por terceros.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Jornada 2022

Generalidades del Riesgo de Fraude

KPMG

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Generalidades del Riesgo de Fraude

Jornada 2022

¿Qué entendemos por riesgo de fraude?

COSO en su Guía para la Administración del Riesgo de Fraude, define el fraude como "*cualquier acto intencional u omisión diseñado para engañar a otros, resultando en que la víctima sufra una pérdida o el perpetrador obtenga una ganancia*."

El Diccionario de Derecho de Black (conocido en inglés como "*Black´s Law Dictionary*") define el fraude como una declaración falsa a sabiendas de la verdad o la ocultación de un hecho material para inducir a otro a actuar en su detrimento.

Según el IAI - *El fraude abarca una gama completa de irregularidades y actos ilegales, caracterizada por un engaño intencionado. El fraude puede ser perpetrado en beneficio o en detrimento de la organización y puede ser efectuado tanto por personas de fuera como de dentro de la misma."*

"Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza."

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Clasificación del Fraude

Jornada 2022

Preparación fraudulenta de información financiera

Eventos de fraude en donde se ejecutan maniobras con el propósito de generar estados financieros que no reflejan adecuadamente la realidad económica de la entidad.

- ✓ Manipulación de gastos/deuda
- ✓ Reconocimiento irregular de ingreso
- ✓ Ocultar gastos no autorizados
- ✓ Disimular u ocultar la aprobación indebida de activos
- ✓ Divulgación de información alterada

Apropiación indebida de activos

Esquemas de fraude en los cuales la persona que lleva a cabo la acción fraudulenta realiza sustracciones de activos o utiliza tales activos u otros recursos de la entidad para beneficio propio.

- ✓ Manipulación de efectivo
- ✓ Robo o mala administración del inventario, equipo o activos
- ✓ Desembolsos fraudulentos
- ✓ Fraude de nómina
- ✓ Préstamos o créditos
- ✓ Fraude en tarjetas o cheques

Actos ilegales y corrupción

Actividades en las que los empleados de una entidad utilizan indebidamente sus influencias para obtener un beneficio personal.

- ✓ Conflictos de interés
- ✓ Sobornos
- ✓ Dádivas ilegales
- ✓ Extorsión
- ✓ Lavado de dinero
- ✓ Falso testimonio

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Triángulo del Fraude

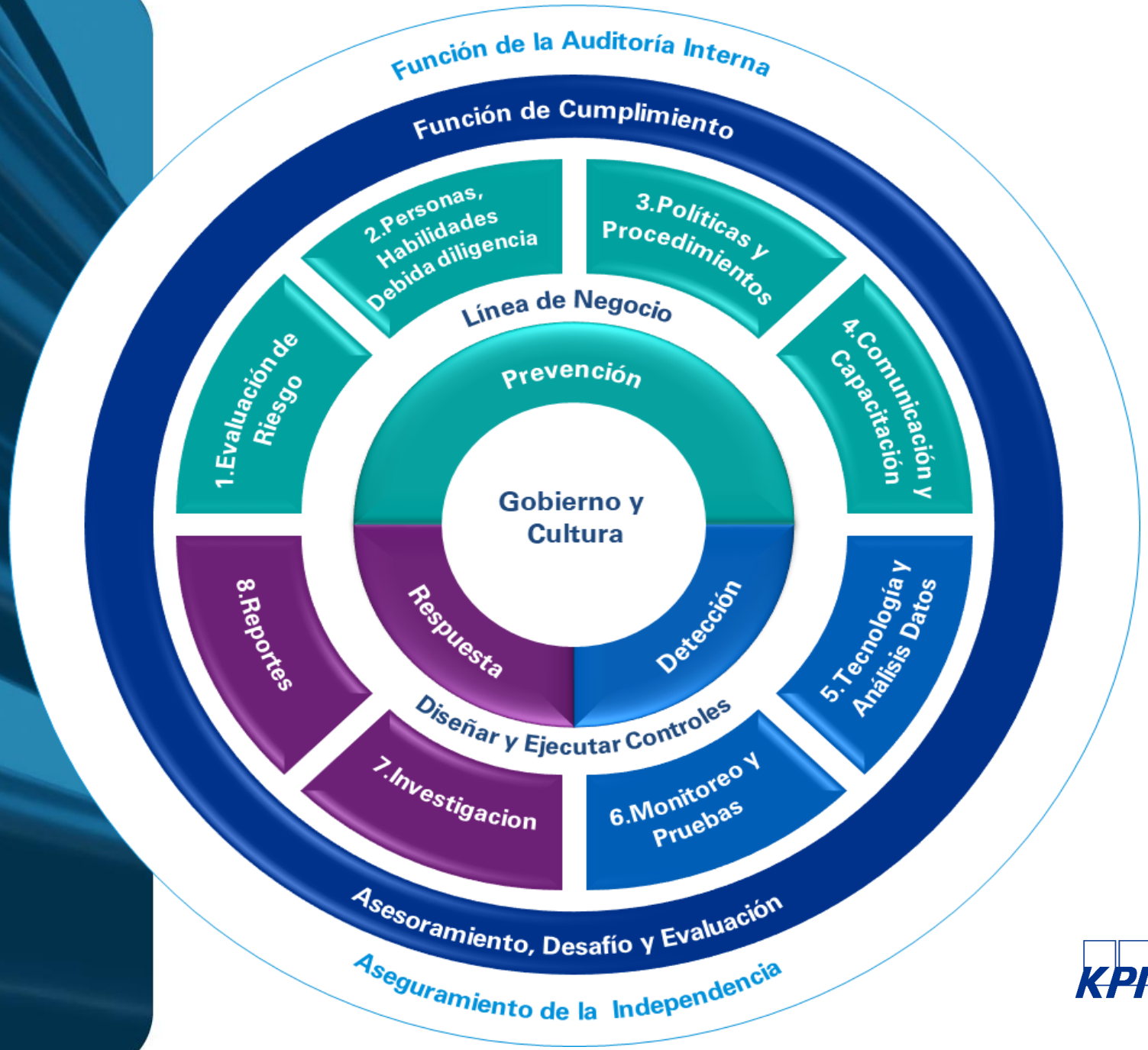
Jornada 2022

- Debilidades en el Gobierno Corporativo
- Ausencia de segregación de funciones
- Concentración de autoridad
- Debilidades en control interno

- Crisis crediticia – deudas
- Enfermedad
- Adicciones

- Valores personales y corporativos
- Venganza
- *"Todos lo hacen"*
- *"Pueden pagarlo"*

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica



Jornada 2022

Gestión del Riesgo de Fraude

KPMG

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Jornada 2022

Generalidades del Riesgo de *Compliance*

KPMG

ISACA Costa Rica Chapter

Instituto de Auditores Internos de Costa Rica

Generalidades del Riesgo de *Compliance*

Jornada 2022

¿Qué entendemos por riesgo de *compliance*?

Riesgo de *compliance*:
ISO 37301:2021 lo define como la probabilidad de ocurrencia y las consecuencias del incumplimiento de las obligaciones de cumplimiento de una organización.

No cumplimiento de *compliance*:

Incumplimiento de las obligaciones de *compliance*.

Obligaciones de *compliance:*
Requisitos que una organización tiene obligatoriamente que cumplir, así como aquellos que una organización elige voluntariamente cumplir.

Debilidades observadas en el mercado:

- Ausencia de la definición de los objetivos de *compliance*
- Identificación de obligaciones de *compliance*
- Pruebas de efectividad de los controles
- Canales de denuncia
- Investigaciones

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Sistema de Gestión de *Compliance* (SGC)

Jornada 2022

El SGC es un marco que integra estructuras, políticas, procesos y procedimientos esenciales para lograr los resultados de cumplimiento deseados, y actuar para prevenir, detectar y responder al incumplimiento.

El marco de un SGC es un asunto estructural: la infraestructura necesaria sobre la cual se construye este sistema luego debe volverse operativo mediante la implementación de políticas, procesos y procedimientos. Asimismo, es necesario mantener y mejorar continuamente el SGC.

El SGC debe basarse en principios de buen gobierno, tales como: proporcionalidad, integridad, transparencia, rendición de cuentas y sostenibilidad.

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Jornada 2022

Espacio para preguntas y/o comentarios

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica

Jornada 2022

Contáctenos

Federico García
Socio
T +(506) 2201-4130
E federicogarcia@kpmg.com

www.kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

KPMG ISACA Costa Rica Chapter Instituto de Auditores Internos de Costa Rica