Control Interno, Optimización de Procesos y Eficiencia Operativa

Por: MF Ramón Miranda Lagunas

COFIDE®
CAPACITACIÓN EMPRESARIAL

Control Interno, Optimización de Procesos y Eficiencia Operativa

Un marco práctico para fortalecer el control, gestionar el riesgo y mejorar la operación

Duración: 4 horas · Dirigido a mandos medios y jefes de área

AL FINALIZAR, USTED PODRÁ:

Objetivos de la conferencia

Comprender el control interno

Su concepto y componentes esenciales.

Aplicar una metodología

8 fases para implementarlo en su área.

Identificar y clasificar riesgos

Que afectan sus procesos críticos.

Diseñar reportes y tableros

Que respalden la rendición de cuentas.

Anticipar tendencias

IA, ciberseguridad y sostenibilidad.

Detectar oportunidades

De optimización y eficiencia operativa.

EL VÍNCULO ENTRE CONTROL Y EFICIENCIA

¿Por qué esta conferencia, y por qué ahora?

- **No son temas separados:** el control interno bien diseñado elimina pasos redundantes y reduce el retrabajo.
- **Los procesos sin control** generan cuellos de botella, duplicidad de esfuerzos y decisiones basadas en información poco confiable.
- **La eficiencia sin control** expone a la organización al fraude, al error y a la pérdida de valor.
- **El equilibrio correcto** protege el patrimonio de la organización y, al mismo tiempo, acelera la operación.

METODOLOGÍA DE HOY

Cómo trabajaremos en esta sesión

Bloques teóricos breves

Directos y aplicables a su realidad operativa.

Casos prácticos en cada módulo

Ejercicios que aterrizan los conceptos vistos.

Discusión grupal

Sus preguntas y experiencias enriquecen la sesión.

Plan de acción personal

Al cierre, se llevará compromisos concretos para su área.

TEMA 1.

CONTROL INTERNO

POR QUÉ IMPORTA

costo de no tener control

5%

de los ingresos anuales se pierde en promedio por fraude ocupacional

12 meses

tarda en promedio una organización en detectar un fraude

83%

de las pérdidas se relacionan con controles débiles, ausentes o vulnerados

Fuente: Association of Certified Fraud Examiners (ACFE), Report to the Nations 2024

DEFINICIÓN DE REFERENCIA (COSO)

Concepto de Control Interno

> *Un proceso, efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos.*
>
> COSO — Committee of Sponsoring Organizations of the Treadway Commission

- Es un proceso continuo, no un evento único
- Lo ejecutan personas, en todos los niveles
- Da seguridad razonable, nunca absoluta

PARA RECORDAR

Ideas clave detrás del concepto

- **Es un proceso continuo,** no un formulario que se firma una vez al año.
- **Involucra a toda la organización,** desde el consejo hasta el colaborador operativo.
- **Se adapta a la estructura** de cada organización — no existe una plantilla única válida para todas.
- **Tiene límites naturales:** ningún sistema de control elimina el 100% del riesgo.

TRES CATEGORÍAS, UN SOLO PROPÓSITO

Objetivos del Control Interno

Eficacia y eficiencia operativa

Uso adecuado de los recursos para cumplir la misión de la organización.

Confiabilidad de la información

Datos íntegros y oportunos para tomar decisiones.

Cumplimiento normativo

Operar dentro del marco legal y regulatorio vigente.

EL MARCO COSO

Los cinco elementos del Control Interno

Ambiente de control

La base de todo: la cultura, los valores y el tono desde la dirección.

Evaluación de riesgos

Identificar y analizar los riesgos que amenazan los objetivos.

Actividades de control

Políticas y procedimientos que aseguran la respuesta al riesgo.

Información y comunicación

Que la información correcta llegue a la persona correcta, a tiempo.

Actividades de supervisión

Evaluaciones continuas o puntuales que confirman que el control funciona.

Ambiente de control: el cimiento

- **Integridad y valores éticos:** el ejemplo de la alta dirección marca la pauta (“tone at the top”).
- **Filosofía y estilo de la dirección:** su actitud frente al riesgo y al control se contagia al resto de la organización.
- **Estructura organizacional:** líneas claras de autoridad y responsabilidad.
- **Competencia del personal** y políticas de recursos humanos coherentes con los valores declarados.

UN CONTROL CLAVE

Segregación de funciones: el principio

Sin segregación de funciones

- Una sola persona autoriza, ejecuta y registra
- Errores y fraudes pasan sin contrapeso
- Difícil detectar desviaciones a tiempo

Con segregación de funciones

- Autorización, ejecución, custodia y registro se reparten
- Un colaborador revisa el trabajo de otro de forma natural
- Se reduce la oportunidad de error y de fraude

SEGREGACIÓN DE FUNCIONES EN LA PRÁCTICA

Las cuatro funciones a separar

Autorización

Quien aprueba la operación.

Ejecución

Quien realiza la operación.

Custodia

Quien resguarda los activos involucrados.

Registro

Quien documenta la operación en los sistemas.

Cuando el equipo es pequeño: controles compensatorios

- **Supervisión directa reforzada** del responsable de área sobre las operaciones críticas.
- **Rotación periódica de tareas** entre colaboradores, para evitar puntos ciegos permanentes.
- **Doble revisión o conciliaciones cruzadas** cuando no es posible separar por completo.
- **Rastros de auditoría (logs)** que permiten reconstruir quién hizo qué y cuándo.

EJERCICIO PRÁCTICO · MÓDULO 1

10 MIN

Caso: el área de compras

En "Comercial del Valle", un mismo colaborador solicita las compras, elige al proveedor, recibe la mercancía y registra la factura en el sistema. No existen políticas escritas de autorización.

SU EQUIPO DEBE:

1. Identifique qué elementos del control interno están ausentes.
2. Proponga cómo segregaría las funciones con el personal disponible (5 personas en el área).
3. Defina un control compensatorio si la segregación total no es posible.

ANTES DE CONTINUAR

Cierre del módulo 1 — para su plan de acción

- ¿Su área tiene un ambiente de control claro, con roles y responsabilidades definidos?
- ¿Puede identificar, hoy mismo, un caso de funciones sin segregar en su equipo?
- ¿Qué control compensatorio podría implementar esta misma semana?

TEMA 2.

FASES PARA IMPLEMENTAR EL CONTROL INTERNO

Implementar control interno es un proceso

- **No se decreta, se construye:** requiere tiempo, comunicación y ajustes constantes.

- **Sigue una secuencia lógica** que va de entender el negocio a mejorar continuamente.

- **Es cíclico, no lineal:** la última fase alimenta de nuevo a la primera.

DE LA CULTURA AL DIAGNÓSTICO

Las 8 fases de implementación (1 de 2)

1

Cultura de control mediante la comunicación

Sensibilizar a toda la organización sobre el porqué y el para qué del control.

2

Recabar información

Levantar procesos, políticas, organigramas y controles existentes.

3

Clasificación de la información

Ordenar lo recabado por proceso, área y nivel de riesgo.

4

Diagnóstico de la información

Analizar las brechas entre lo que existe y lo que debería existir.

Las 8 fases de implementación (2 de 2)

5

Revisión de procedimientos

Actualizar o rediseñar procedimientos con base en el diagnóstico.

6

Evaluación del control interno y de gestión

Medir si los controles diseñados realmente funcionan en la operación.

7

Implementación, seguimiento y adecuación

Poner en marcha los controles y ajustarlos sobre la marcha.

8

Evaluación, retroalimentación y adecuación (continuo)

Cerrar el ciclo: lo aprendido alimenta la siguiente vuelta del proceso.

PROFUNDIZANDO EN LAS FASES 1-2

Fase 1 y 2: cultura e información

Comunique el “para qué”

El control protege el trabajo de las personas, no las vigila.

Involucre a los dueños del proceso

Quien participa en el diseño, se apropia del control.

Recabe evidencia real

Entreviste, observe la operación, revise los formatos usados en la práctica.

PROFUNDIZANDO EN LAS FASES 3-4

Fase 3 y 4: clasificar y diagnosticar

Clasifique por proceso y riesgo

Agrupe la información por macroproceso y nivel de criticidad.

Compare contra un marco de referencia

Use COSO u otro marco reconocido como vara de medición.

Documente brechas, no solo hallazgos

Cada brecha debe ligarse a un riesgo y a un objetivo de negocio.

Fase 5 y 6: procedimientos y evaluación

Rediseñe antes de controlar

Un procedimiento ineficiente con un control encima sigue siendo ineficiente.

Pruebe el control, no solo su diseño

Un control bien diseñado que nadie ejecuta no protege nada.

Mida con indicadores simples

Cumplimiento, tiempo de ciclo, tasa de error: pocos, bien elegidos.

PROFUNDIZANDO EN LAS FASES 7-8

Fase 7 y 8: implementar y sostener

Implemente de forma gradual

Priorice los controles de mayor riesgo primero; no todo a la vez.

Dé seguimiento con fechas y responsables

Sin dueño y sin fecha, la adecuación no ocurre.

Cierre el ciclo con retroalimentación

Lo evaluado en la fase 8 alimenta la siguiente vuelta de la fase 1.

LO QUE HAY QUE EVITAR

Errores comunes al implementar

Error frecuente

- Copiar controles de otra organización sin adaptarlos
- Diseñar controles sin probarlos en la operación real
- Implementar todo a la vez, sin priorizar
- Tratarlo como un proyecto con fecha de cierre

Consecuencia típica

- Controles que no encajan con la operación y se ignoran
- Cuellos de botella o controles que nadie sigue
- Saturación del equipo y resistencia al cambio
- El sistema se deteriora en cuanto termina el “proyecto”

EJERCICIO PRÁCTICO · MÓDULO 2

10 MIN

Caso: diagnóstico exprés

Su equipo debe levantar y diagnosticar el proceso de "reembolso de gastos de viaje" en dos semanas, antes de rediseñarlo.

SU EQUIPO DEBE:

1. Liste 3 fuentes de información que recabaría (fase 2).
2. Proponga un criterio de clasificación para ordenar lo recabado (fase 3).
3. Mencione una brecha típica que esperaría encontrar en el diagnóstico (fase 4).

Del control al proceso: la conexión con la eficiencia

- **Cada fase es también una oportunidad de mejora de proceso,** no solo de control.
- **El diagnóstico (fase 4) suele revelar pasos redundantes,** no solo riesgos.
- **La revisión de procedimientos (fase 5)** es el momento natural para simplificar, automatizar o eliminar actividades sin valor.

Cierre del módulo 2 — para su plan de acción

- ¿En qué fase del ciclo se encuentra hoy el control interno de su área?
- ¿Qué información necesitaría recabar primero si empezara mañana?
- ¿Qué procedimiento de su equipo merece una revisión urgente?

R E C E S O

Al regreso: Módulo 3 · Administración de Riesgos

TEMA 3.

ADMINISTRACIÓN DE RIESGOS

PUNTO DE PARTIDA

¿Qué es un riesgo?

> *La posibilidad de que ocurra un evento que afecte negativamente el logro de los objetivos de la organización.*

Definición operativa, con base en el marco COSO ERM

- Siempre se define con relación a un objetivo
- Se mide con dos variables: probabilidad e impacto
- También puede representar una oportunidad no aprovechada

Riesgo y control: dos caras de la misma moneda

- **El riesgo justifica el control:** no se diseñan controles porque sí, se diseñan para mitigar un riesgo identificado.

- **Sin evaluación de riesgos,** el control interno es genérico: igual para una operación crítica que para una trivial.

- **El control de riesgos no busca eliminar el riesgo,** busca llevarlo a un nivel aceptable (“apetito de riesgo”).

ANTES DE IDENTIFICAR RIESGOS

Entendimiento del negocio: el punto de partida

Modelo de negocio

¿Cómo genera valor la organización y de qué depende ese valor?

Entorno externo

Mercado, competencia, regulación, condiciones económicas.

Objetivos estratégicos

Los riesgos solo tienen sentido en relación con lo que se quiere lograr.

SEIS CATEGORÍAS A VIGILAR

Tipos de riesgo

Estratégico

Decisiones que afectan la dirección de largo plazo.

Operativo

Fallas en procesos, personas o sistemas del día a día.

Financiero

Liquidez, crédito, tipo de cambio, tasas de interés.

De cumplimiento

Incumplir leyes, normas o contratos aplicables.

Tecnológico

Fallas de sistemas, obsolescencia, dependencia de terceros.

Reputacional

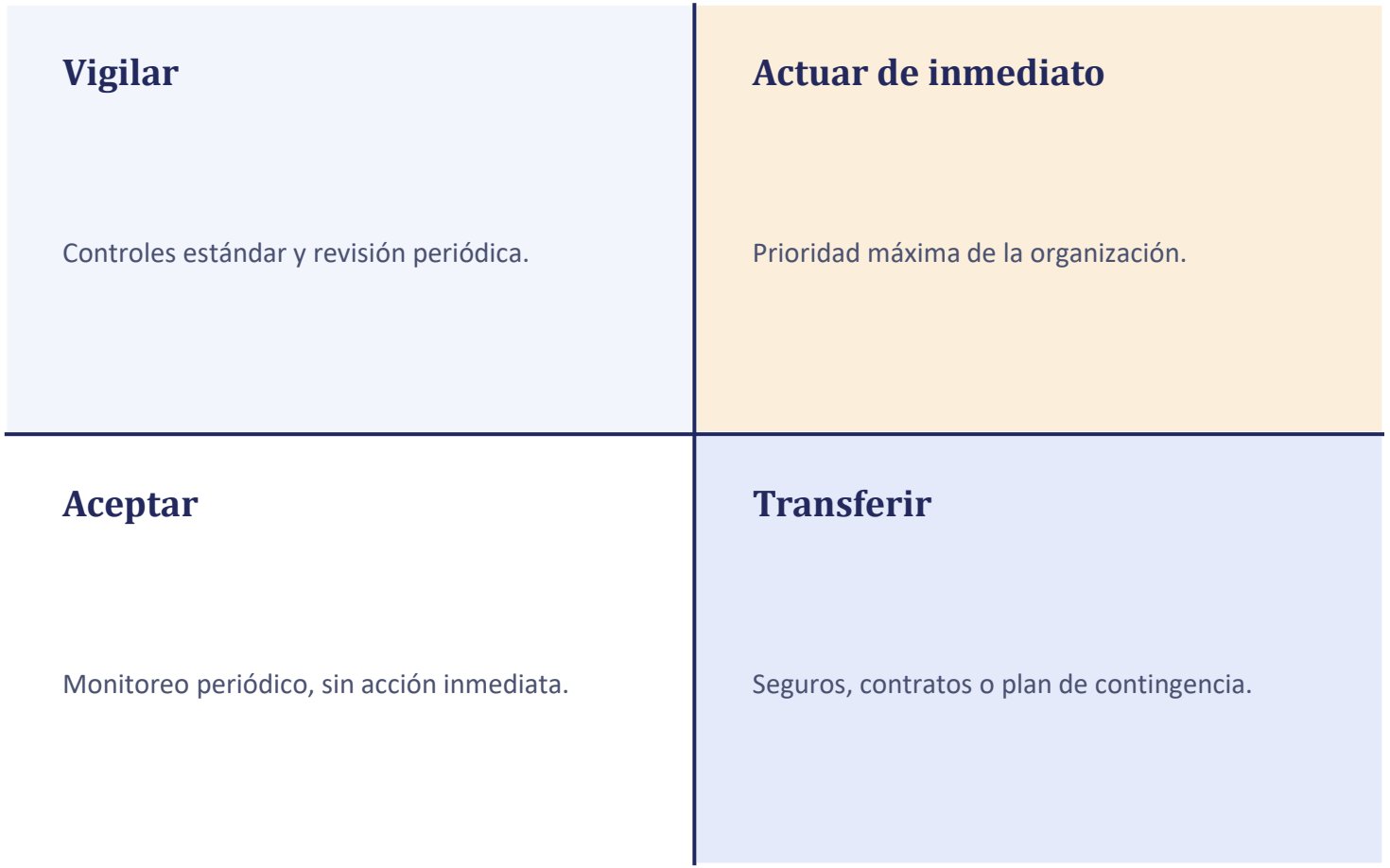
Pérdida de confianza de clientes, inversionistas o la sociedad.

Identificación de riesgos: técnicas prácticas

- **Talleres con dueños de proceso:** quien ejecuta el proceso conoce mejor que nadie sus puntos débiles.
- **Análisis de incidentes pasados:** lo que ya falló una vez puede volver a fallar.
- **Revisión de indicadores y quejas:** las desviaciones en los datos anticipan problemas.
- **Benchmarking sectorial:** riesgos que ya enfrentaron organizaciones similares.

MATRIZ DE PRIORIZACIÓN

Priorizar con probabilidad e impacto



LAS 4 RESPUESTAS AL RIESGO

Estrategias para proteger y reducir el riesgo

Evitar

Eliminar la actividad que genera el riesgo cuando su costo supera el beneficio.

Reducir / mitigar

Implementar controles que bajen la probabilidad o el impacto.

Transferir

Trasladar el riesgo a un tercero: seguros, contratos, tercerización.

Aceptar

Asumir el riesgo conscientemente cuando está dentro del apetito definido.

Construir una cultura de gestión de riesgos

- **El riesgo es responsabilidad de todos,** no solo del área de auditoría o cumplimiento.

- **Hablar de riesgos debe ser seguro,** no motivo de sanción — de lo contrario, nadie los reporta a tiempo.

- **Revisar el mapa de riesgos periódicamente:** el negocio cambia, y los riesgos cambian con él.

EJERCICIO PRÁCTICO · MÓDULO 3

12 MIN

Caso: mapa de riesgos de su área

Piense en un proceso crítico de su área (por ejemplo: nómina, ventas, producción o atención a clientes).

SU EQUIPO DEBE:

1. Identifique 2 riesgos reales de ese proceso.
2. Clasifique cada uno por tipo (estratégico, operativo, financiero, cumplimiento, tecnológico, reputacional).
3. Ubique cada riesgo en la matriz de probabilidad e impacto y proponga una estrategia de respuesta.

ANTES DE CONTINUAR

Cierre del módulo 3 — para su plan de acción

- ¿Su área cuenta con un mapa de riesgos actualizado?
- ¿Qué riesgo de alta prioridad no tiene todavía una estrategia de respuesta clara?
- ¿Con quién debería hablar esta semana para entender mejor un riesgo del negocio?

TEMA 4.

INFORMES, REPORTES Y RENDICIÓN DE CUENTAS

¿Por qué reportar bien es parte del control?

- **Un control que no se reporta** no se puede evaluar ni mejorar.

- **La rendición de cuentas genera confianza:** interna, con la dirección, y externa, con accionistas, reguladores y clientes.

- **Reportar no es “exhibir errores”:** es dar visibilidad para tomar mejores decisiones.

EL REPERTORIO DEL CONTROL INTERNO

Cinco formas de rendir cuentas

Reportes operativos

El pulso diario o semanal de la operación.

Dictámenes de auditoría

La opinión formal e independiente sobre el estado del control.

Tableros de control

La vista ejecutiva, visual, casi en tiempo real.

Reporte de hallazgos

Lo que se encontró y no debería estar pasando.

Planes de remediación

El compromiso concreto de corregir, con fecha y responsable.

Características de un buen reporte operativo

- **Oportunos:** reflejan la operación reciente, no la de hace un mes.
- **Accionables:** cada dato lleva a una decisión o a una pregunta concreta.
- **Consistentes:** mismas métricas, mismo formato, periodo tras periodo — permiten comparar.
- **Dirigidos a su audiencia:** el nivel operativo necesita detalle; la dirección necesita síntesis.

Dictámenes de auditoría: qué comunican

- **Alcance:** qué se evaluó y qué quedó fuera de la revisión.
- **Criterio:** contra qué marco o norma se comparó (COSO, políticas internas, ley aplicable).
- **Opinión:** el nivel de seguridad razonable que se puede dar sobre lo evaluado.
- **Limitaciones:** toda auditoría tiene alcance y recursos limitados — se declaran, no se ocultan.

Tableros de control: la vista ejecutiva

- **Pocos indicadores, bien elegidos:** un tablero con 40 métricas no es un tablero, es un reporte disfrazado. Máximo 10 indicadores
- **Semaforización clara:** rojo, amarillo, verde, con criterios objetivos y conocidos por todos.
- **Actualización confiable:** un tablero desactualizado destruye la confianza en todo el sistema.
- **Enlazado a la decisión:** cada semáforo en rojo debe tener un responsable y una acción asociada.

Cómo comunicar lo que se encontró

- **Describa el hecho, no la intención:** qué pasó, con evidencia, sin suponer motivos.
- **Vincule el hallazgo a un riesgo y a un control:** explique por qué importa, no solo qué ocurrió.
- **Clasifique por severidad:** no todos los hallazgos requieren la misma urgencia de respuesta.
- **Involucre al responsable del área** antes de formalizar el reporte, siempre que sea posible.

PLANES DE REMEDIACIÓN

De hallazgo a solución

1

Confirmar el hallazgo

Validar el hecho con evidencia suficiente y con el área responsable.

2

Identificar la causa raíz

Preguntar “por qué” varias veces hasta llegar al origen real.

3

Definir la acción correctiva

Concreta, medible y con un responsable único.

4

Dar seguimiento hasta el cierre

Verificar que la acción se implementó y que fue efectiva.

EJERCICIO PRÁCTICO · MÓDULO 4

10 MIN

Caso: del hallazgo al plan de remediación

La auditoría interna encontró que, en los últimos 3 meses, el 20% de las órdenes de compra se autorizaron después de haberse recibido la mercancía.

SU EQUIPO DEBE:

1. Redacte el hallazgo en una frase clara, basada en el hecho.
2. Proponga una hipótesis de causa raíz.
3. Defina una acción correctiva con responsable y plazo.

ANTES DE CONTINUAR

Cierre del módulo 4 — para su plan de acción

- ¿Los reportes de su área generan decisiones, o solo se archivan?
- ¿Existe un mecanismo claro de seguimiento a los planes de remediación?
- ¿Qué hallazgo pendiente en su equipo merece atención esta semana?

TEMA 5.

TENDENCIAS Y RETOS FUTUROS

POR QUÉ ESTE MÓDULO IMPORTA

El control interno no es estático

- **Los marcos como COSO no cambian todos los años,** pero el entorno en el que se aplican sí.

- **La tecnología crea riesgos** y herramientas de control al mismo tiempo.

- **Anticiparse es más barato que reaccionar:** actualizar el sistema de control antes de la crisis, no después.

EL MAPA DE ESTE MÓDULO

Cuatro fuerzas que redefinen el control interno

Control interno en la era digital

Procesos, evidencia y controles cada vez más automatizados.

Ciberseguridad

El riesgo tecnológico como riesgo de negocio central.

Inteligencia artificial

Nueva herramienta de control y, a la vez, nuevo riesgo a controlar.

Sostenibilidad

La información ESG entra al mismo estándar de rigor que la financiera.

Control interno en la era digital

- **La evidencia ya no es solo en papel:** registros de sistemas, huellas digitales y metadatos.

- **Los controles automatizados reducen el error humano,** pero concentran el riesgo en la configuración del sistema.

- **La auditoría continua** reemplaza gradualmente a la auditoría por muestreo periódico.

TEMA 2 DE 4 · TENDENCIAS 2026

Ciberseguridad: prioridad de consejo

- **La ciber-resiliencia es el enfoque central:** no se trata solo de evitar el ataque, sino de mantener la operación mientras ocurre.

- **La automatización defensiva con IA** gana protagonismo: detección de anomalías en tiempo real y respuesta automatizada.

- **La presión regulatoria integra la ciberseguridad a la gobernanza:** deja de ser un tema solo técnico y pasa a reportarse al consejo de administración.

Inteligencia artificial: herramienta y riesgo

Como herramienta de control

Analiza el 100% de las transacciones y detecta patrones anómalos.

Como riesgo a gestionar

Sesgos algorítmicos, dependencia excesiva y decisiones difíciles de explicar.

Como reto de gobernanza

Requiere estrategia y marco de gobernanza definidos antes de escalar su uso.

Sostenibilidad: la información ESG bajo el mismo rigor

- **La información de sostenibilidad enfrenta el mismo reto** que antes enfrentaba la financiera: fragmentación y poca confiabilidad.

- **COSO extendió su marco de control interno a la información de sostenibilidad,** con los mismos cinco componentes y diecisiete principios del control financiero.

- **La exigencia regulatoria y de los grupos de interés va en aumento:** prepararse hoy facilita el cumplimiento mañana.

DE LA TENDENCIA A LA ACCIÓN

Qué significa esto para su rol, hoy

- **No necesita ser experto en IA o ciberseguridad:** necesita saber qué preguntas hacer a quienes sí lo son.

- **Incluya estos riesgos en su mapa de riesgos** del módulo 3 — no los trate como temas aparte.

- **Empiece pequeño:** un piloto de automatización de un control, o una política básica de manejo de datos.

EJERCICIO PRÁCTICO · MÓDULO 5

10 MIN

Caso: un riesgo emergente en su organización

Elija uno de los cuatro temas del módulo: digitalización, ciberseguridad, inteligencia artificial o sostenibilidad.

SU EQUIPO DEBE:

1. Identifique una forma en que ese tema ya afecta o afectará a su área.
2. Ubique ese riesgo en la matriz de probabilidad e impacto del módulo 3.
3. Proponga una primera acción, pequeña y concreta, para los próximos 30 días.

Cierre del módulo 5 — para su plan de acción

- ¿Qué tan preparada está su área frente a estos cuatro temas, del 1 al 10?
- ¿Con quién de tecnología, seguridad o sostenibilidad debería empezar a hablar?
- ¿Cuál es su primera acción concreta de aquí a 30 días?

CIERRE
Y
CONCLUSIONES

Las cinco ideas que no debe olvidar

- **Control interno** es un proceso continuo de personas, no un documento estático.
- **Implementarlo** sigue 8 fases que se repiten en ciclo, no una sola vez.
- **El riesgo** da sentido y prioridad a cada control que se diseña.
- **Reportar bien** cierra el ciclo y sostiene la rendición de cuentas.
- **El futuro** (digital, ciber, IA, sostenibilidad) ya está aquí — prepararse es más barato que reaccionar.

Su plan de acción de 30-60-90 días

- **30 días:** un diagnóstico rápido de control y un mapa de riesgos inicial de su área.

- **60 días:** al menos un control compensatorio o rediseño de proceso implementado.

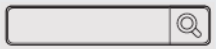
- **90 días:** un primer reporte o tablero que muestre el avance a su equipo y a su jefatura.

Fuentes y referencias

- COSO — Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (coso.org)
- ACFE — Report to the Nations 2024, Association of Certified Fraud Examiners
- COSO — Internal Control over Sustainability Reporting (ICSR): guidance summarized by EY (ey.com)
- KPMG Tendencias — “Auditoría basada en agentes de IA” (tendencias.kpmg.es, 2026)
- KPMG Costa Rica — “Consideraciones en Ciberseguridad 2026” (kpmg.com/cr)
- Computing.es — “Resiliencia, automatización y gestión del riesgo: claves de la ciberseguridad en 2026”

POR SU ATENCIÓN ¡GRACIAS!

CONTÁCTANOS



PÁGINA WEB

www.cofide.mx

TELÉFONO

01 (55) 46 30 46 46

DIRECCIÓN

Av. Río Churubusco 594 Int. 203,
Col. Del Carmen Coyoacán, 04100
CDMX

SIGUE NUESTRAS REDES SOCIALES

COFIDE

Cofide SC

Cofide SC

@cofide.mx