



Evaluación de Controles bajo COSO 2013

De la verificación documental a la
mitigación real del riesgo

ALGERisk Corporation | Generando Cultura de Riesgos

Guía de transformación operativa para auditores y gestores de riesgo.

La Ilusión del Control: El peligro del “Check de Auditoría”

Marcar que un control “existe” o “se ejecutó” no significa que mitigue el riesgo para el cual fue diseñado.

La Realidad Operativa:

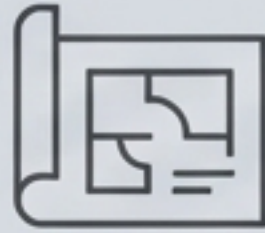
- Confundir la evaluación con un trámite genera una falsa sensación de seguridad.
- El riesgo sigue presente en la operación, solo que ahora está “mejor documentado”.

El imperativo COSO 2013: Los controles deben ser probados en su capacidad real de protección, no solo en su existencia formal.



El Marco Conceptual: Eficacia vs. Efectividad

EFICACIA DEL CONTROL (En el Papel)



El control “hace sentido” lógicamente.

- ✓ • Está correctamente diseñado.
- ✓ • Responde al riesgo identificado.
- ✓ • Existe formalmente.
- ✓ • Tiene responsable, frecuencia y procedimiento definido.

El Salto de
Calidad COSO

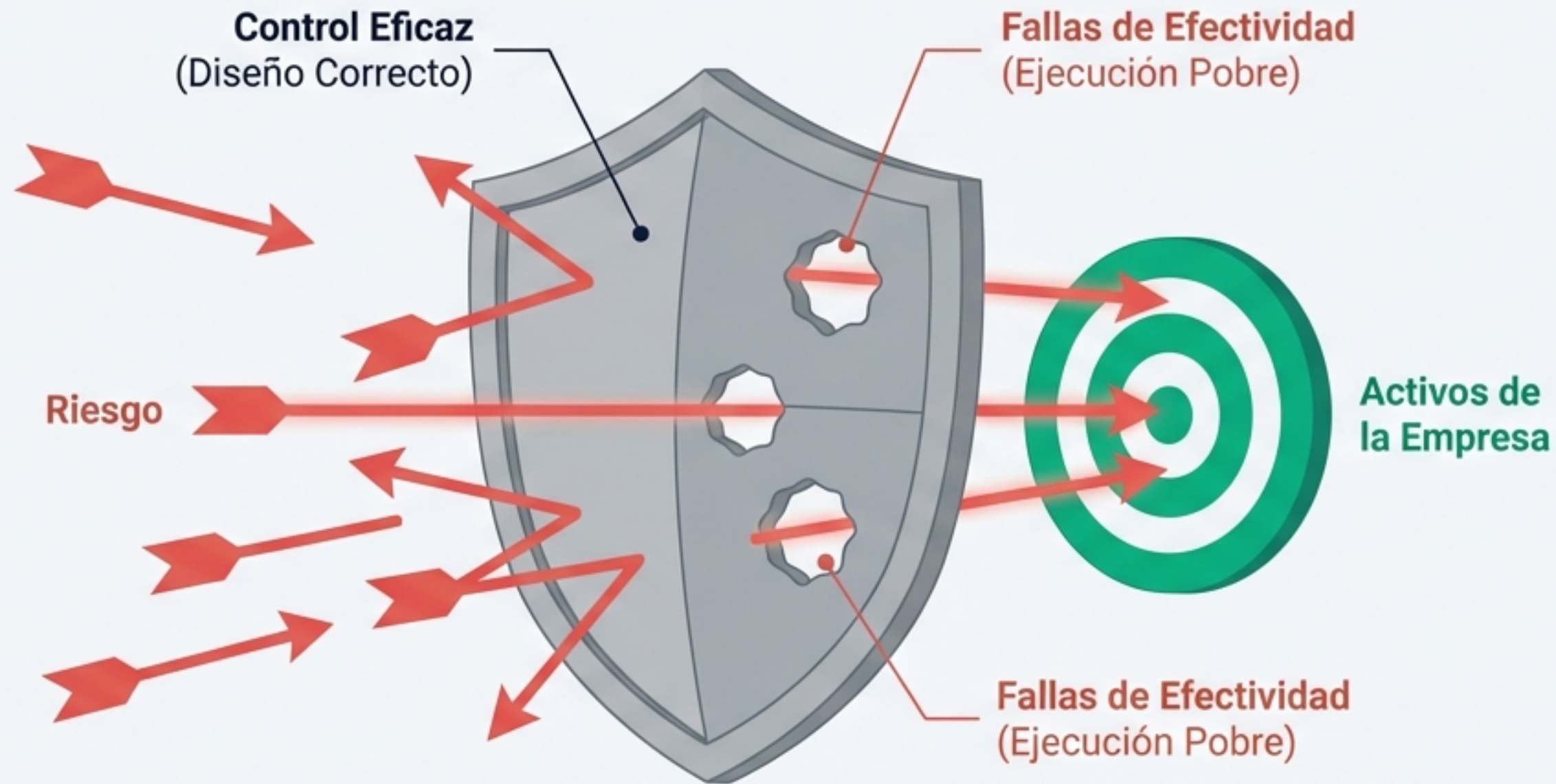
EFFECTIVIDAD DEL CONTROL (En la Realidad)



El control protege a la organización.

- ✓ • Se ejecuta consistentemente.
- ✓ • Reduce la probabilidad o el impacto real.
- ✓ • Funciona en condiciones reales, no ideales.
- ✓ • Evita o detecta eventos relevantes.

La Brecha de Protección



Insight Central

Un control puede ser eficaz (bien diseñado), pero no efectivo.

Un control no efectivo **no protege** a la organización, aunque esté documentado y aprobado.

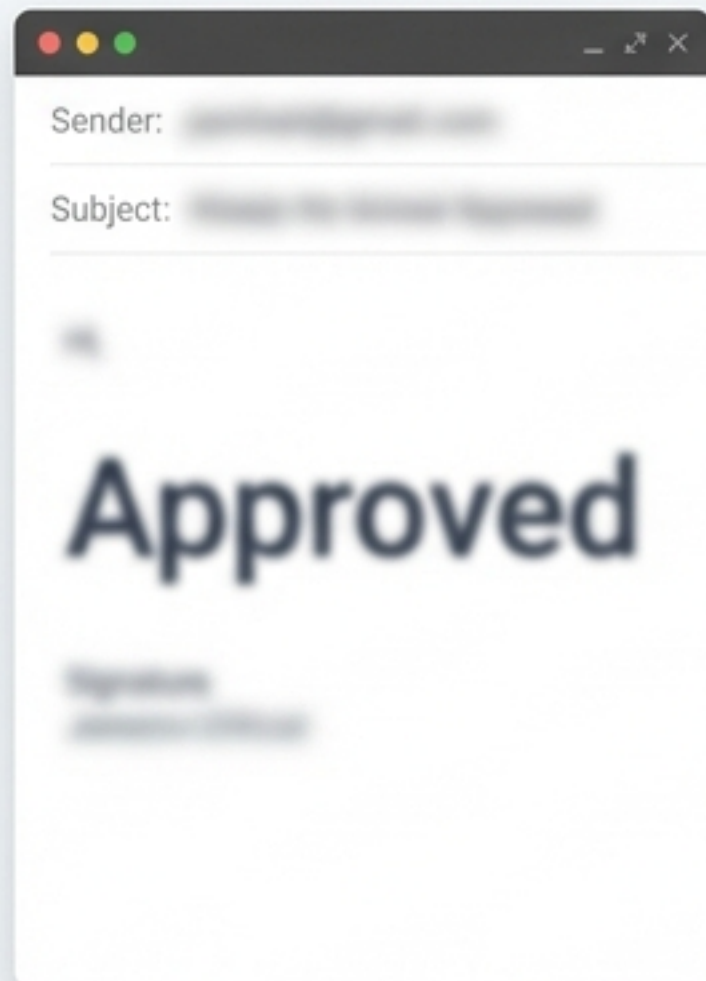
COSO 2013 exige evaluar ambas dimensiones. Quedarse solo en el diseño es negligencia operativa.

Calidad de la Evidencia: Más allá del “Pantallazo”

Sustancia sobre forma para demostrar mitigación.



Evidencia Débil o Irrelevante (La Trampa)



- Correos genéricos sin hilo de decisión.
- Pantallazos recortados sin contexto (fecha/hora/sistema).
- Documentos sin trazabilidad.
- Firmas sin validación real del contenido.

Sirve para “cerrar el hallazgo”, pero no prueba nada.



Evidencia Suficiente y Relevante (Estándar COSO)

- Demuestra inequívocamente que el control se ejecutó.
- Permite verificar cómo se ejecutó (la lógica aplicada).
- Está vinculada directamente al riesgo mitigado.
- Es trazable y reproducible por un tercero.

Timestamp: 2023-10-27 14:30:45 UTC
Transaction ID: TX-987654321
Digital Signature ID: Digitally Signed: J.Doe / ID 12345
Action: Control Executed / Validation Passed
Parameters: Value > Threshold: Yes / Confirmed

Checklist de Validación de Evidencia

La pregunta no es "¿Hay evidencia?". La pregunta es: "¿Esta evidencia prueba que el riesgo fue controlado?"



1. Ejecución Real

¿El documento confirma la acción, no solo la intención?



2. Vínculo al Riesgo

¿Queda claro cómo esta acción redujo el impacto o probabilidad?



3. Reproducibilidad

¿Podría otro auditor llegar a la misma conclusión solo viendo este documento?



4. Contexto

¿La evidencia incluye fecha, responsable y datos del sistema?



Fase 1: Pruebas de Diseño (La Teoría)

Evaluar la arquitectura del control antes de verificar su operación.



Concepción: ¿Está bien pensado el control? ¿Ataca la causa raíz?



Cobertura: ¿Cubre el riesgo correcto o uno adyacente?



Proporcionalidad: ¿Es el esfuerzo del control proporcional al impacto del riesgo?



Dependencia: ¿Depende excesivamente del juicio de una persona (falible)?

Diagnostic Question: ¿Este control, si se ejecuta exactamente como está diseñado, podría mitigar el riesgo?

Fase 2: Pruebas de Funcionamiento (La Práctica)

Verificar la ejecución en el mundo real, donde las personas fallan y los procesos se estresan.

- ✓ **Oportunidad:** ¿Se ejecuta cuando corresponde (tiempo y forma)?
- ✓ **Responsable:** ¿Lo ejecuta quien tiene la autoridad y conocimiento?
- ✓ **Calidad:** ¿Se ejecuta con la profundidad esperada?
- ✓ **Consistencia:** ¿Se mantiene en el tiempo o es esporádico?



La Regla de Oro

Un control bien diseñado que no se ejecuta es un control inexistente.

Error Común: Probar diseño una sola vez y asumir funcionamiento automático.

Monitoreo: Indicadores Dinámicos de Control

Si no medimos los controles, no sabemos si siguen funcionando.

Indicadores Mal Usados (Estáticos)



Indicadores Mal Usados (Estáticos)

- Solo miden **cumplimiento** documental.
- Métricas **binarias** de 'Sí/No'.
- Ausencia de **umbrales de alerta**.
- Ejemplo **inútil**: "El control se ejecutó".

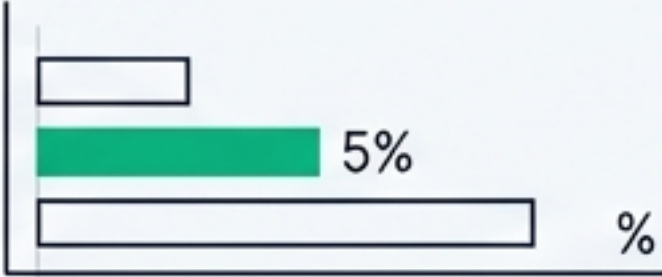
Indicadores Útiles (Dinámicos)



Indicadores Útiles (Dinámicos)

- Miden **tendencias**, no solo eventos aislados.
- **Alertan** sobre **degradación** del control.
- Permiten **escalar** decisiones al Comité de Riesgos.

Ejemplos Prácticos de KPIs según COSO

Dimension	KPI Description	Visual Micro-chart
Frecuencia de Fallas	% de excepciones detectadas por el control.	 A horizontal bar chart with a green bar representing 5% of the total length. The label '5%' is placed next to the bar, and a '%' symbol is at the end of the axis.
Impacto Residual	Número de eventos no detectados (fugas). Variación del riesgo residual a lo largo del tiempo.	 A line chart on a grid background. A green line starts at a high point on the left, slopes down to the middle, stays flat for one unit, and then slopes down again to the bottom right, ending with an arrowhead.
Eficiencia	Tiempo promedio de corrección tras la detección.	 A circular clock icon with a green hand pointing to the 2 o'clock position. To its right is a horizontal bar chart with a green bar and the label '2 Hrs'.

Estos indicadores permiten anticipar fallas y ajustar controles antes de que el riesgo se materialice.

Conclusión: Evaluar para Proteger, no para Cumplir

El control interno no es un trámite; es una herramienta de gestión real. COSO 2013 no promueve controles para la auditoría, sino controles que funcionen cuando el entorno cambia, las personas fallan o los procesos se estresan.

Call to Action:

Si los controles no se evalúan más allá del 'check', la organización permanece vulnerable.

Objetivo Final: Pasar de la ilusión del control a la realidad operativa.