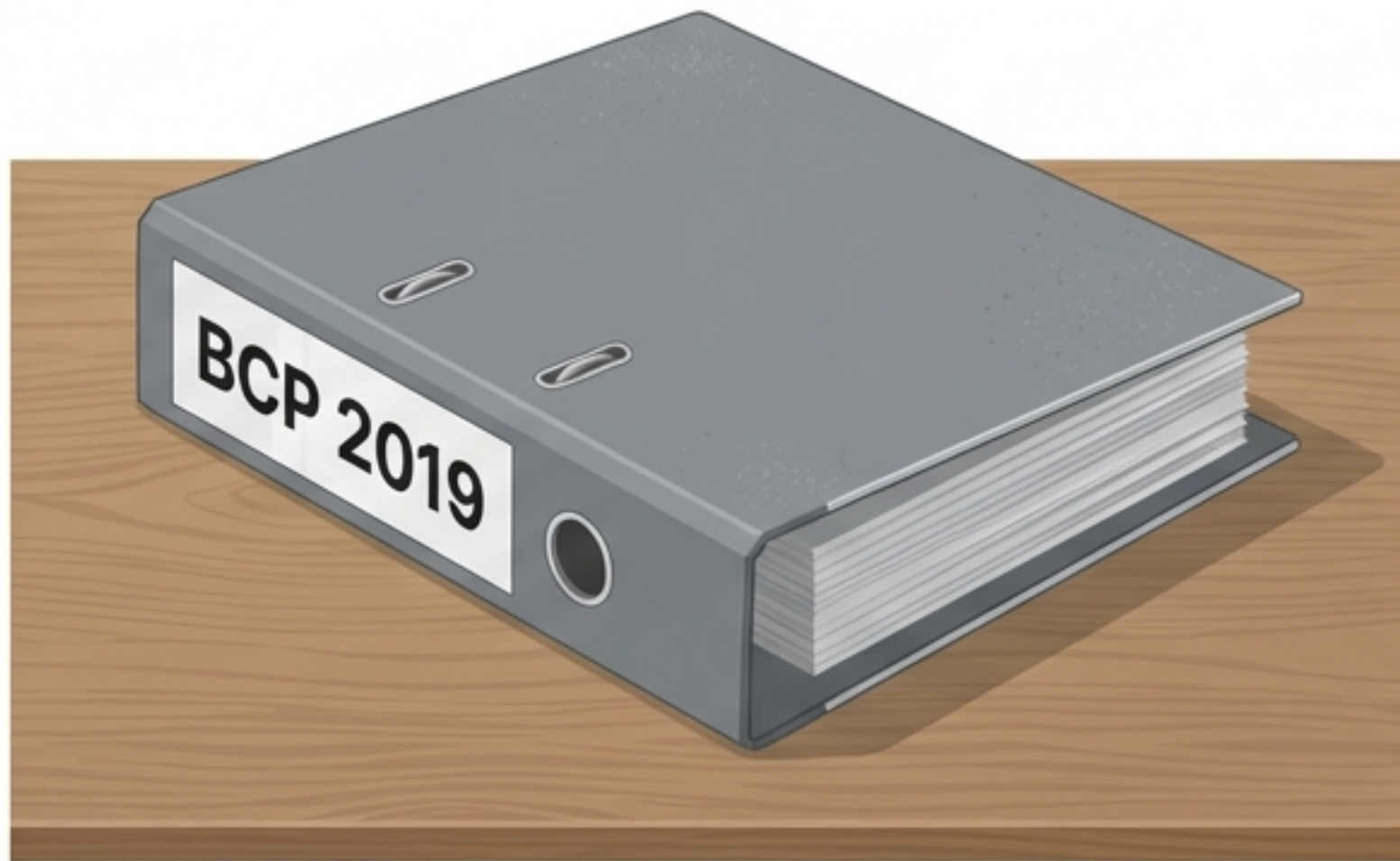
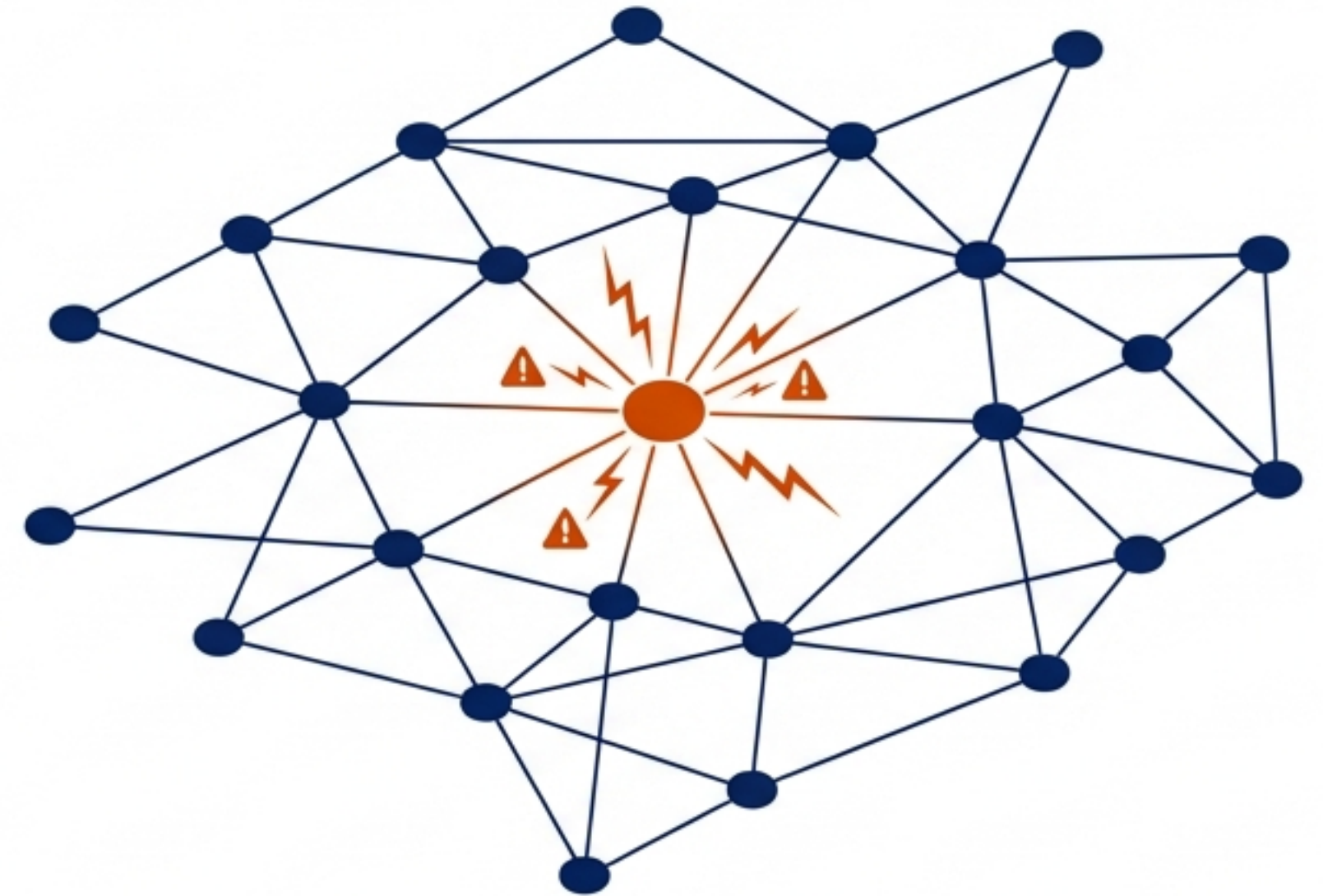




Generando Cultura de Riesgos: Continuidad en Entornos Digitales



Por qué los BCP tradicionales están fallando y cómo transitar hacia la Resiliencia Operacional.

Un podcast de ALGERisk Corporation

Cumplimiento no es sinónimo de capacidad: La paradoja de la continuidad moderna

El Problema

Las organizaciones tienen BCP documentados y pruebas periódicas, pero siguen fallando ante interrupciones digitales.



La Causa

Los planes fueron diseñados para desastres físicos, no para ecosistemas Cloud, dependencias SaaS y riesgos sistémicos.



El Veredicto

El entorno cambió, pero la estrategia de continuidad no.



Inter Regular

El BCP tradicional cumple con la norma, pero no funciona bajo presión digital.

El enfoque clásico se diseñó para un mundo estable, físico y bajo control directo

■ Foco en lo Físico

Diseñado para incendios, indisponibilidad de oficinas y fallas de infraestructura local.

■ Supuesto de Control

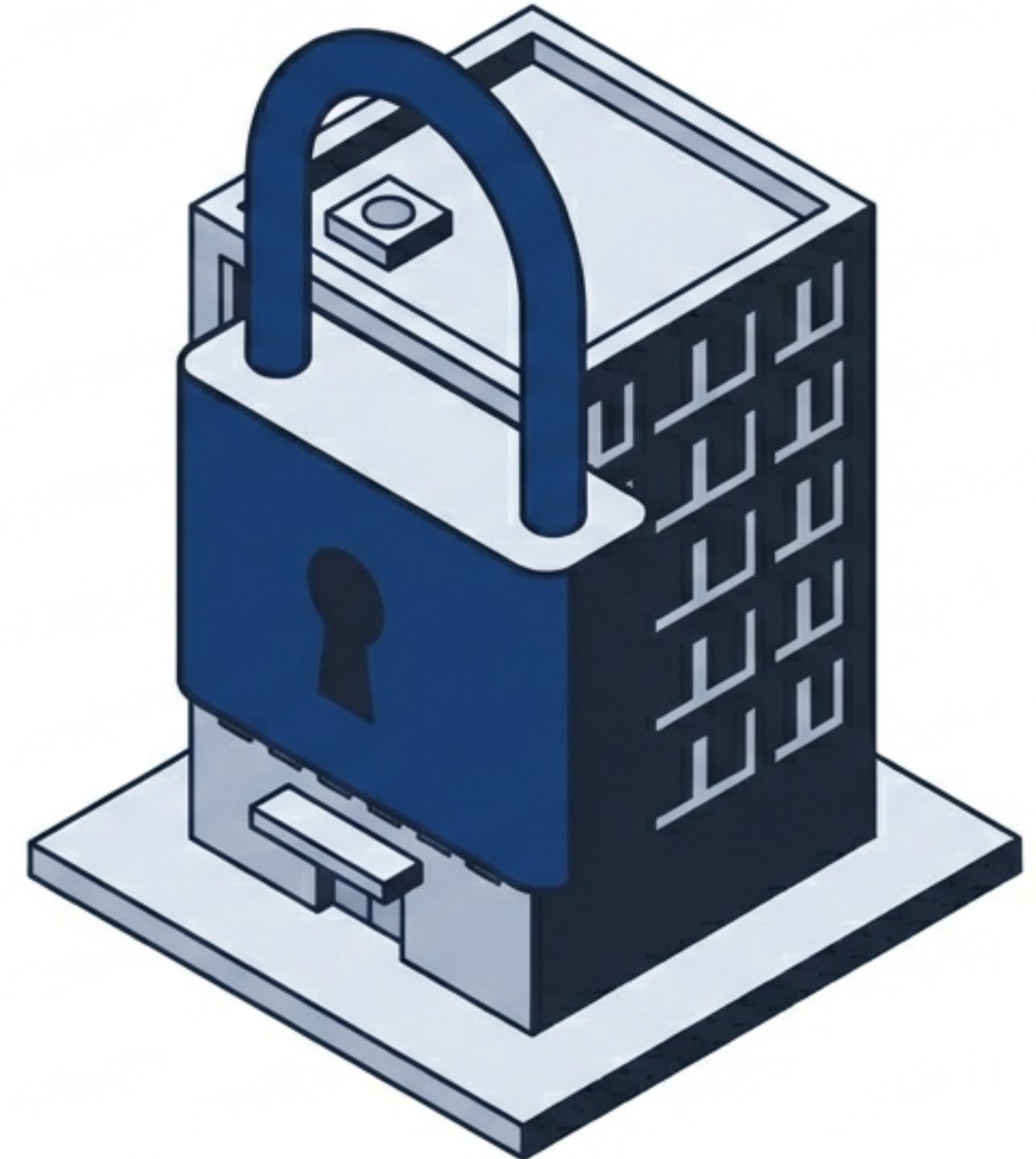
Asume que la organización es dueña de la infraestructura y puede repararla.

■ Escenarios Estáticos

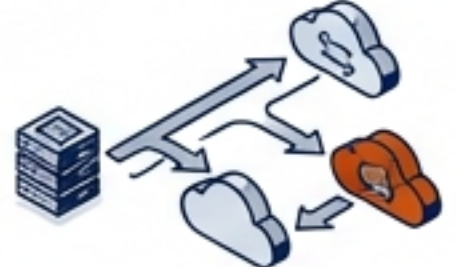
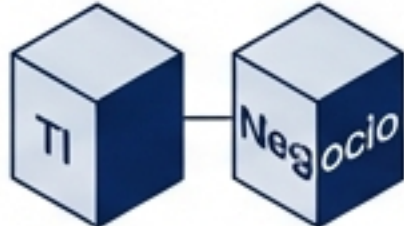
Se basa en riesgos predecibles que no evolucionan en tiempo real.

■ Metodología Manual

Depende de recuperación manual de procesos que hoy son imposibles de operar sin sistemas.



Los incidentes actuales no respetan los límites físicos ni organizacionales

	BCP Tradicional	Realidad Digital
Amenaza	Desastre Físico / Falla Local 	Ciberataque / Caída de SaaS Global 
Respuesta	Mover gente a sitio alternativo 	Redirigir tráfico digital / Cambiar proveedor 
Control	Infraestructura propia 	Arquitectura de Terceros (Nube) 
Gestión	Silos (TI separado del Negocio) 	Gestión Integrada de Crisis 

Key Insight: No se puede ‘trasladar’ la operación a un sitio de respaldo si el proveedor global de nube está caído.

La nube no es infalible: Entendiendo la trampa de la responsabilidad compartida



El Mito

- La nube siempre está disponible
- El proveedor se encarga de la continuidad.

La Realidad y Requerimientos

- ⚠️ Usted no controla la arquitectura.
- ⚠️ Los incidentes pueden ser regionales o globales.
- ⚠️ Los SLAs son compensaciones financieras, no soluciones operativas.

Análisis de Single Points of Failure

Análisis de Single Points of Failure



Estrategias Multi-cloud reales

Estrategias Multi-cloud reales



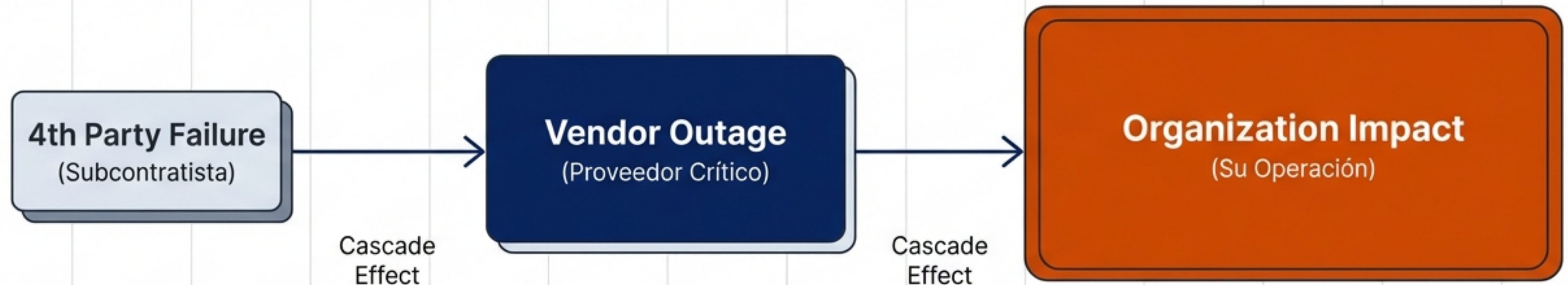
Planes de salida y portabilidad de datos

Planes de salida y portabilidad de datos



Usted hereda los riesgos que no gestiona: La crisis de la cadena de suministro

La dependencia de Fintechs, integradores y operadores Cloud introduce riesgos que el BCP suele ignorar.



Strategic Fix: Alineación total entre BCP y TPRM (Third Party Risk Management).
Si no hay planes alternativos viables para proveedores críticos, no hay continuidad.

El papel aguanta todo, la operación no: La brecha del RTO

RTO Teórico (El Deseo)



4 Hours

Definido sin análisis técnico, no validado con proveedores, desconectado del impacto real.

RTO Realista (La Capacidad)



4 Days

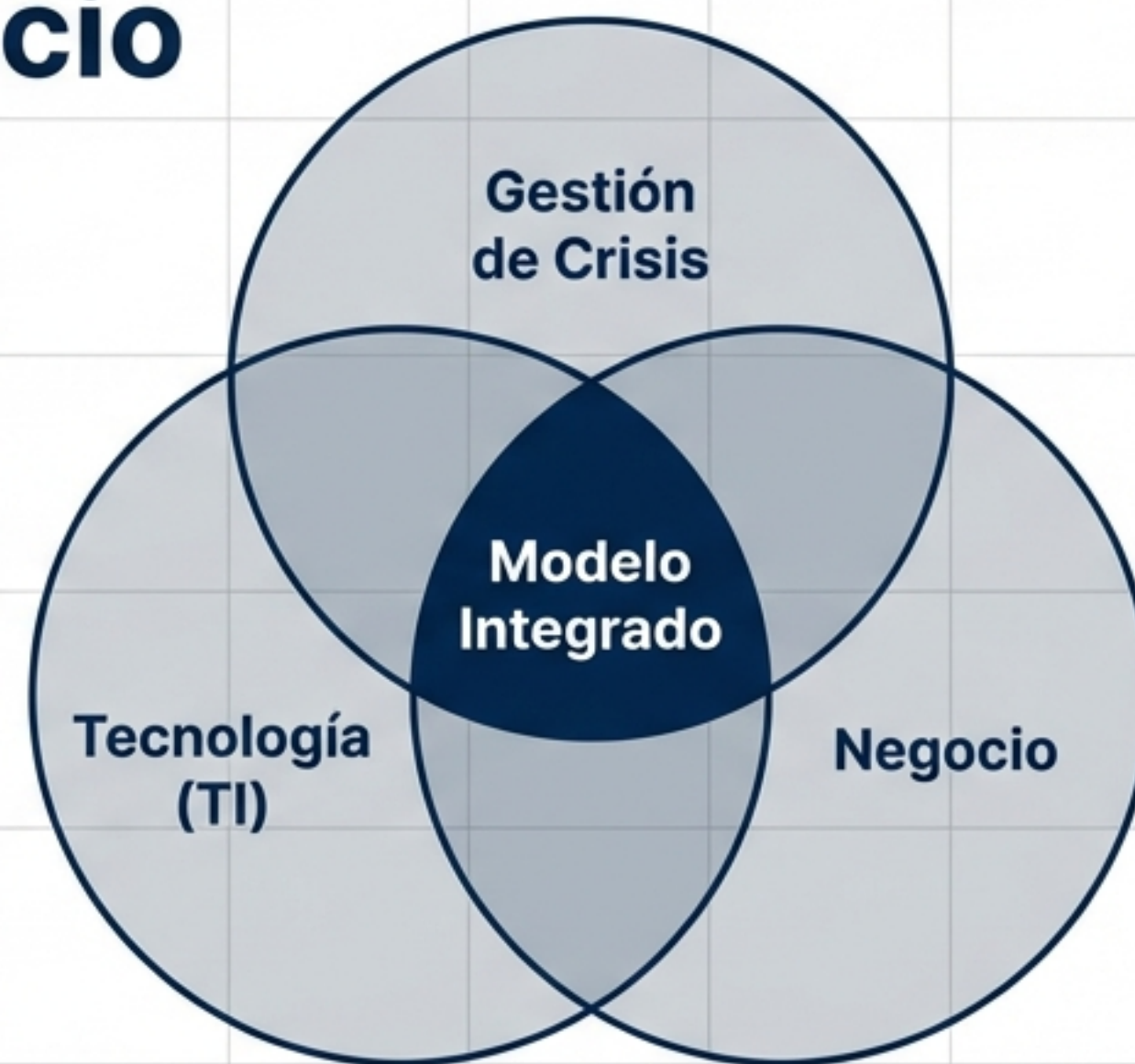
Basado en pruebas de estrés, alineado al apetito de riesgo, validado con TI.

"El tiempo real de recuperación define la magnitud de la crisis, no el tiempo escrito en el plan."

La continuidad moderna exige la integración de Crisis, Tecnología y Negocio

La separación artificial entre la recuperación de TI y la Gestión de Crisis del negocio es inviable.

- Disrupción Súbita y compleja
- Alto impacto reputacional inmediato
- Presión regulatoria instantánea

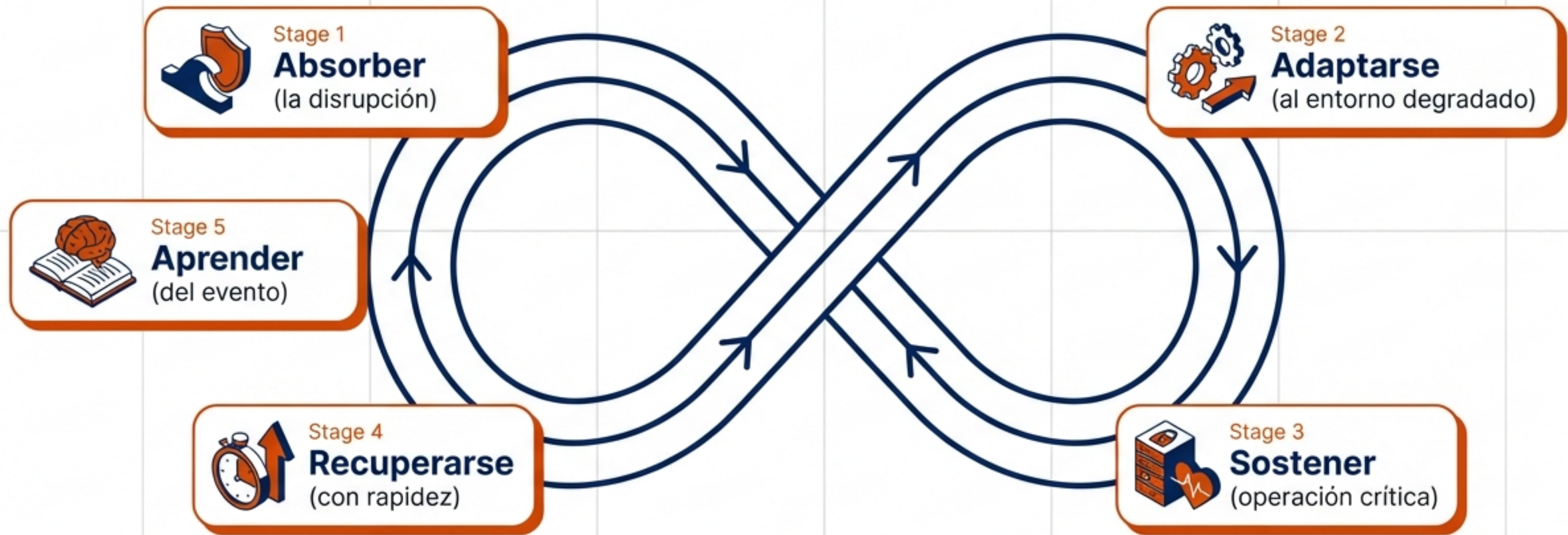


Insight Block

Activación temprana de comités + Decisiones coordinadas + Priorización financiera.

Más allá del BCP: Hacia una Resiliencia Operacional Digital

Dejar de pensar en “Cumplir auditoría” y pasar a “Capacidad de supervivencia”.



Convergencia: Unifica Ciberseguridad, Riesgo Tecnológico, TPRM y Gobierno Corporativo.

Hoja de ruta para modernizar la continuidad del negocio

1

Validación Técnica

Someter los RTOs a pruebas de estrés real (no simulacros de escritorio).

2

Integración TPRM

Clasificar proveedores críticos y exigir planes de contingencia conjuntos.

3

Estrategia Cloud

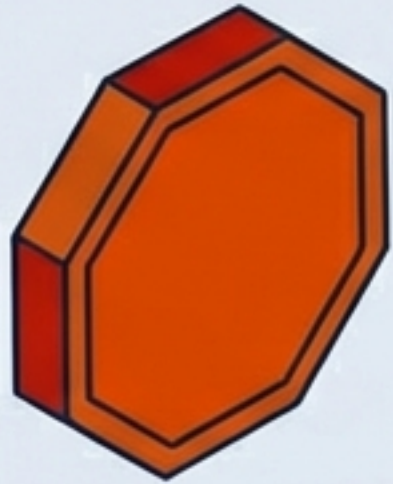
Revisar contratos para incluir portabilidad y estrategias de salida.

4

Gobierno de Crisis

Entrenar a los ejecutivos en la toma de decisiones bajo incertidumbre digital.

La continuidad ya no es un ejercicio documental, es una capacidad estratégica



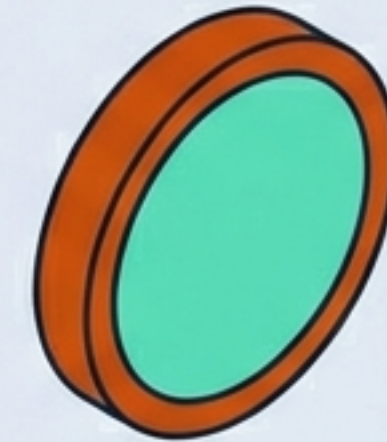
STOP (Rojo)

Asumir que la nube nunca falla y confiar en RTOs teóricos.



CAUTION (Amarillo)

Tratar la continuidad como un silo aislado de TI o Ciberseguridad.



GO (Verde)

Desarrollar Resiliencia
Desarrollar Resiliencia Operacional Digital integrada con proveedores y gestión de crisis.

Transformando cumplimiento en capacidad real.

ALGERisk Corporation

Basado en el episodio “Continuidad en entornos digitales”
del podcast *Generando Cultura de Riesgos*

Las organizaciones que sigan tratando la continuidad como un documento estarán expuestas. La **resiliencia** es su mejor ventaja competitiva.