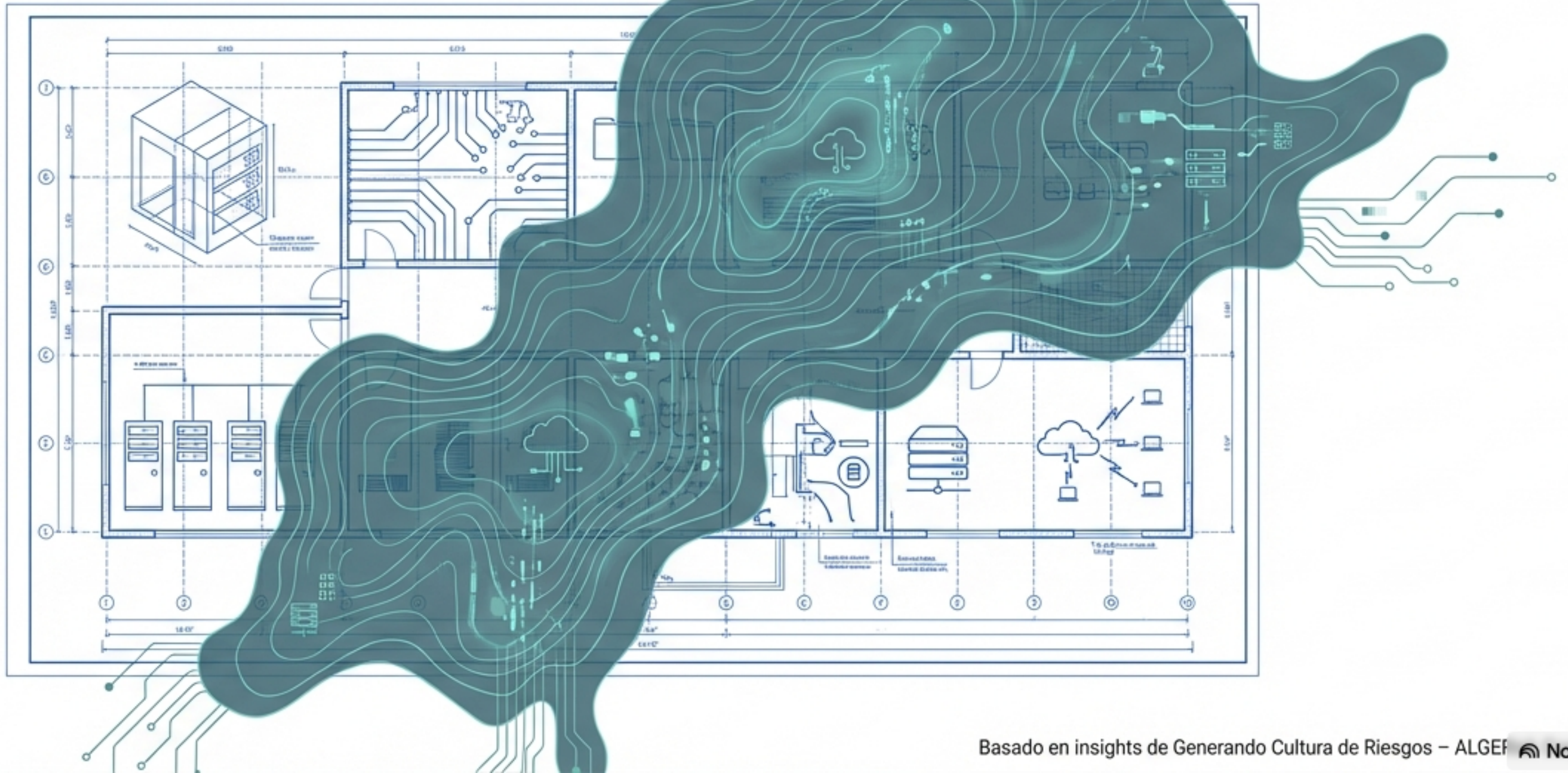


DRP Tradicional vs. Entornos Digitales

Por qué los planes de recuperación fallan cuando el core del negocio no es tuyo.



La ilusión de seguridad: Planes certificados que no responden



Durante años, las organizaciones han invertido recursos masivos en diseñar Planes de Recuperación ante Desastres (DRP). Están documentados, probados y certificados.



El problema no es la falta de planificación, sino que estamos usando mapas diseñados para un territorio que ya no existe.

El DRP tradicional se construyó sobre supuestos obsoletos.

El modelo clásico fue diseñado bajo tres pilares que hoy han desaparecido en la práctica moderna:



1. Infraestructura Propia

El hardware vivía en un data center físico bajo llave.



2. Control Directo

El equipo interno tenía acceso total a servidores y respaldos.



3. Procesos Centralizados

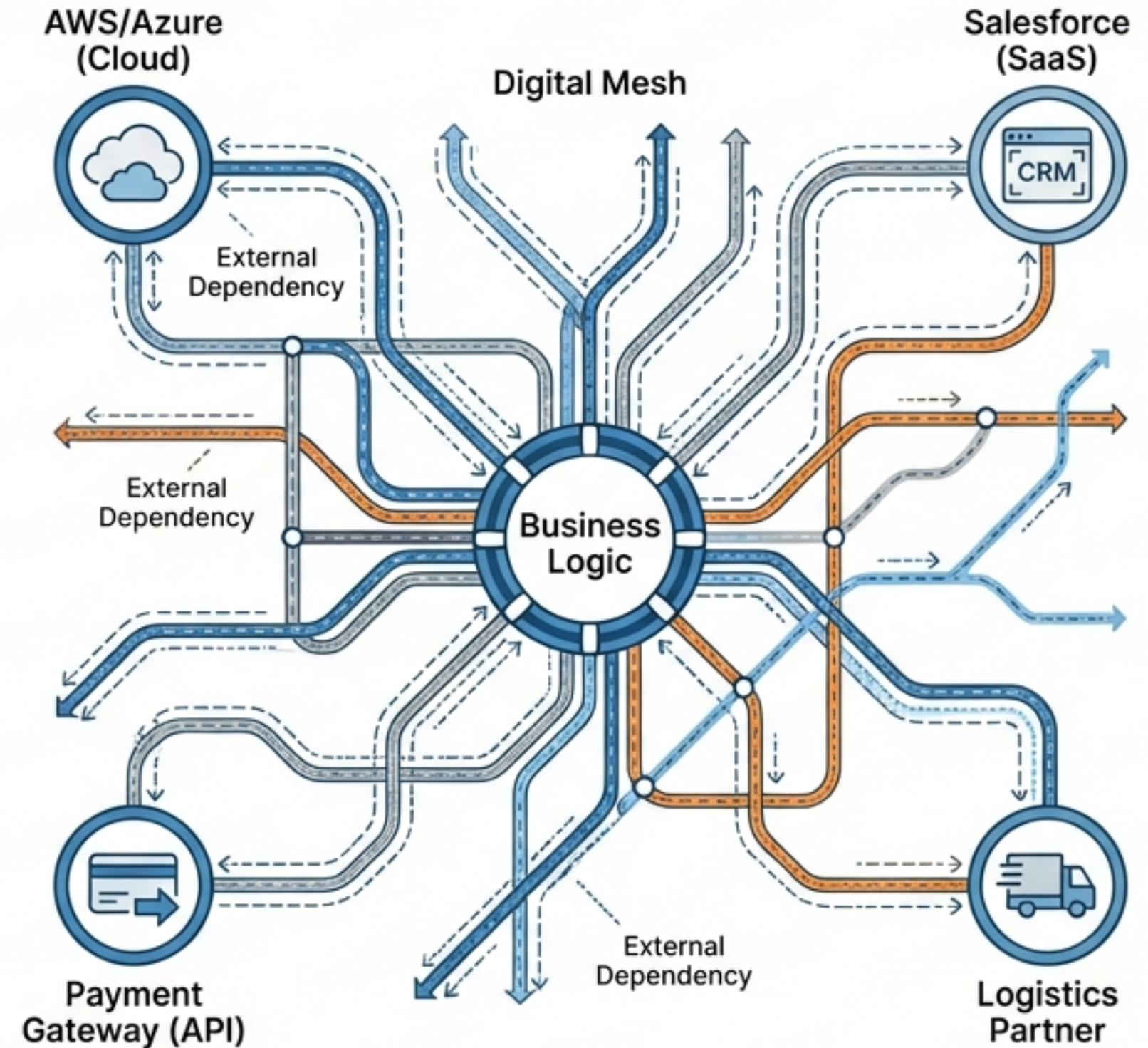
La recuperación era una tarea técnica aislada dentro de TI.

Este modelo solo funciona cuando el entorno es estable y el riesgo es puramente físico.

La nueva realidad: Un ecosistema distribuido y dependiente.

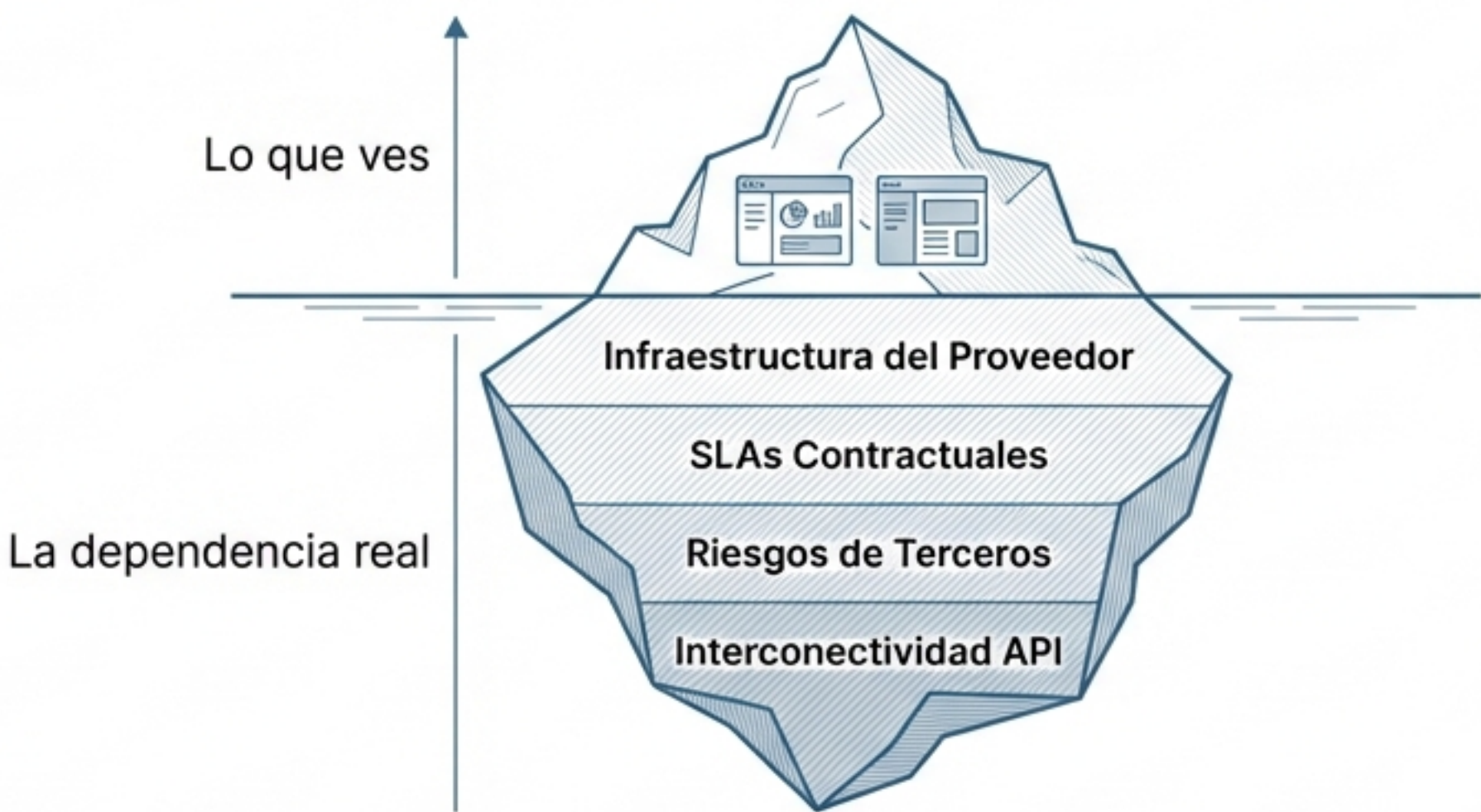
En un entorno digital, el DRP deja de ser un problema técnico de “restauración” para convertirse en un riesgo estratégico.

- **El Core en la Nube:** Infraestructura distribuida (Cloud, Multi-cloud).
- **Dependencia Crítica:** El negocio se apoya en SaaS, Fintechs y plataformas de terceros.
- **El Tejido Digital:** Integraciones complejas vía APIs que conectan el ecosistema.



La Brecha de Gobernanza: Ya no controlas tu recuperación.

Cuando el servicio es SaaS o Cloud, la organización pierde la capacidad de intervención directa.



Antes (Control Técnico)	Ahora (Gestión de Terceros)
Reiniciar un servidor, restaurar una cinta.	Dependencia de contratos, SLAs, y la capacidad de respuesta de proveedores externos.

La recuperación ya no depende de las manos de tu equipo de TI,
sino de las cláusulas firmadas con tus socios.

La trampa de las métricas teóricas (RTO y RPO).

Uno de los mayores errores actuales es mantener objetivos de recuperación definidos en el vacío, sin validación externa.



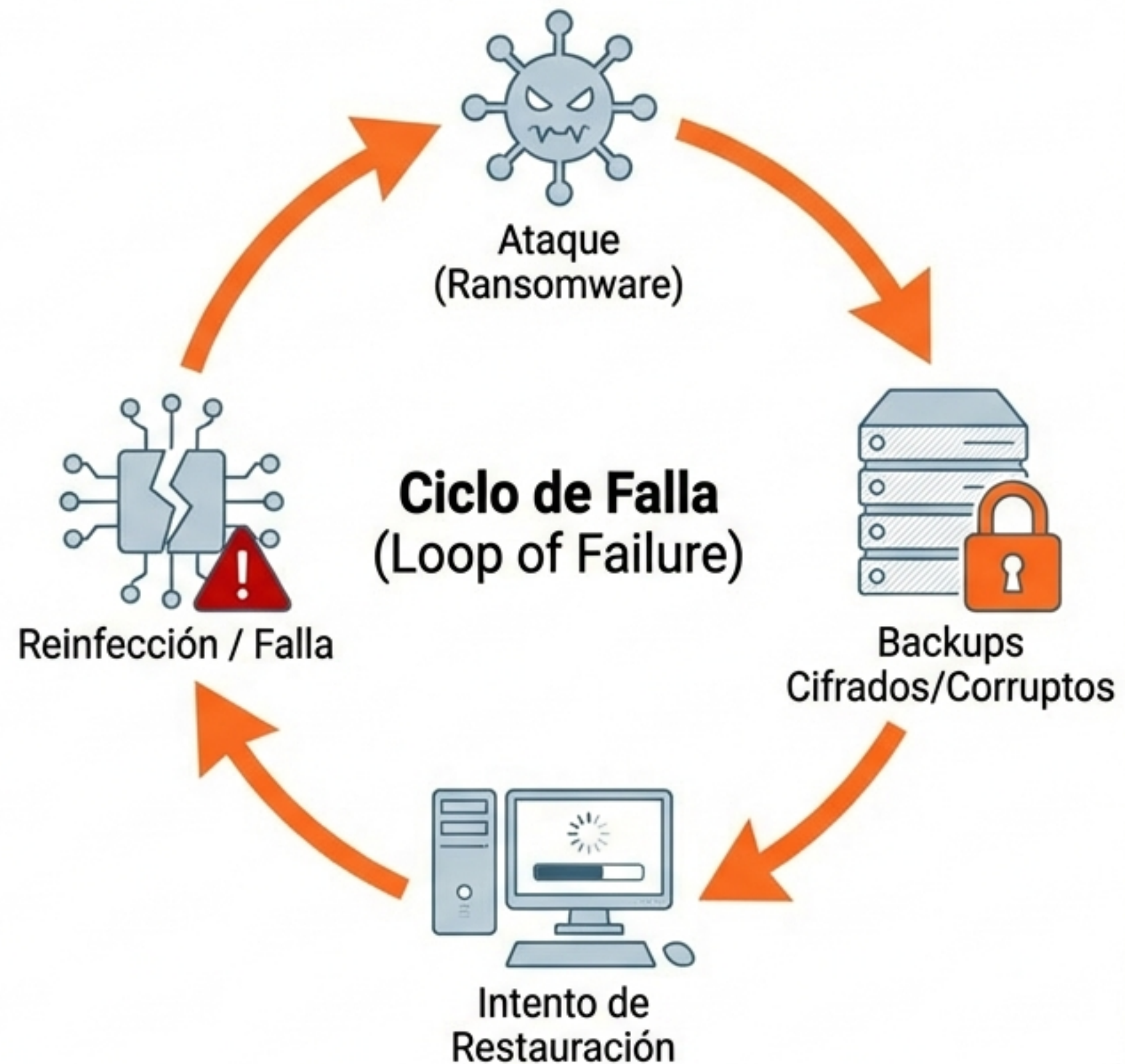
- **RTO Irreal:** Definido sin considerar los tiempos de respuesta del proveedor SaaS.
- **RPO vs. Ransomware:** La integridad de los datos importa más que la frecuencia del respaldo.
- **Dependencias No Mapeadas:** El sistema 'A' se recupera, pero falla porque el sistema 'B' (externo) sigue caído.

El sistema vuelve a estar en línea, pero el negocio no puede operar.

El punto ciego: Ciberincidentes y corrupción de datos.

El DRP tradicional asume un fallo físico, no un adversario activo.

- **Respaldos Comprometidos:** Los atacantes cifran o corrompen los backups antes de atacar.
- **Restauración sin Forense:** Reiniciar sistemas sin análisis previo destruye evidencia y permite la persistencia del atacante.
- **Ataques a la Cadena de Suministro:** El incidente entra a través de un proveedor confiable.



De la recuperación técnica a la resiliencia del negocio.

En entornos digitales, el DRP debe integrarse con disciplinas que antes operaban separadas.



El nuevo mandato: DRP como capacidad, no como documento.

Enfoque en Servicios Digitales

Roboto Serif

Proteger flujos de valor completos, no solo activos de hardware aislados.



Validación Extendida

Roboto Serif

Realizar pruebas conjuntas con proveedores críticos, no solo simulacros internos.



Simulación de Decisiones

Roboto Serif

Involucrar a la Alta Dirección para probar la toma de decisiones bajo presión, no solo el reinicio de sistemas.



Métricas de Resiliencia

Roboto Serif

Medir la capacidad de absorber el golpe y continuar, no solo la velocidad técnica de restauración.



Recuperar la Recuperar la capacidad de operar.

*El problema no es que las organizaciones no tengan DRP.
El problema es que siguen usando planes diseñados para
un mundo que ya no existe.*

En la era digital, recuperarse ya no es solo restaurar la tecnología;
es recuperar la capacidad de decidir, responder y sobrevivir.
En se girtador es unfitamentarales conipetas para erscnar 'la
oapala de técnco de ALGERisk Corporation.

Generando Cultura de Riesgos – ALGERisk Corporation