Más allá del 'cloud' de papel: lecciones coreanas para infraestructuras a prueba de desastres

Madrid, 9 de octubre de 2025 – **Stackscale**, proveedor europeo de infraestructura de cloud privado y bare-metal del Grupo Aire, publica un análisis técnico del incendio en el centro de datos del NIRS en Corea del Sur y comparte recomendaciones prácticas para diseñar plataformas resilientes con **geo-redundancia** y **copias de seguridad inmutables**. El documento pone foco en cómo evitar puntos únicos de fallo y alinear la continuidad de negocio con buenas prácticas verificables.

Diseño y resiliencia: el eje del análisis

"Lo ocurrido en Corea no es un problema de 'cloud', sino de **arquitectura**", subraya **David Carrero**, cofundador de Stackscale. "Una nube real implica **redundancia geográfica**, **automatización de réplicas** y **recuperación ante desastres**. Si un desastre local puede borrar tu servicio, se ha construido un punto único de fallo". El caso del NIRS evidenció almacenamiento monolítico, ausencia de réplicas externas y concentración de **96 sistemas críticos** en un único dominio de fallo.

De 3-2-1 a 3-2-1-1-0

El análisis recuerda que la estrategia **3-2-1** (tres copias, dos soportes, una fuera de sitio) debe evolucionar a **3-2-1-1-0**: añadir **1 copia "air-gapped"** y asegurar **0 errores** mediante pruebas periódicas de restauración. Las bandas de ransomware ya atacan no solo producción, sino también copias conectadas a red.

Recomendación operativa de Stackscale

"La mejor póliza son varias", explica Carrero. "**Producción activo-activo** en dos centros de datos para **RPO=0** y **RTO=0**, y **backups inmutables** en un **tercer emplazamiento**". La diferencia entre activo-activo y activo-pasivo está en el tiempo de respuesta: el primero **sobrevive al fallo de inmediato**; el segundo requiere conmutación y suele ser más económico.

Backups inmutables y software

En entornos Stackscale se recomiendan soluciones con **retención WORM**, **verificación de restauraciones** y **alertas de anomalías**. Para escenarios open source, **Proxmox Backup Server** aporta incrementales, deduplicación, compresión Zstandard y sincronización local/remota con licencia **AGPLv3**; también se integran plataformas comerciales como **Veeam** cuando aplica. "La clave no es el software, es el **diseño** y **probar las recuperaciones**: sin test, no hay plan de recuperación", concluye Carrero.

Checklist mínimo de resiliencia (orientativo)

- **Dos ubicaciones** para producción.
- **Backups en un tercer DC** con WORM o **air-gap**.
- **RPO/RTO definidos** y **ensayados**.
- **Restauraciones probadas** cada 3–6 meses.
- **Segregación de credenciales** con **MFA**.
- **Monitorización de anomalías**.
- **Cumplimiento** (ENS / ISO 27001).

“La infraestructura resiliente no se construye con marketing, sino con **disciplina de ingeniería**. Es lo que evita que, cuando arde un centro de datos, se queme también nuestra memoria digital”, remata Carrero.

Sobre Stackscale

Stackscale es una empresa europea del **Grupo Aire** con presencia en **centros de datos** en Madrid y Ámsterdam. Ofrece **cloud privado**, **servidores dedicados**, **almacenamiento con georeplicación síncrona** y **servicios gestionados** para cargas críticas que exigen rendimiento, previsibilidad de costes y soberanía del dato.