Más allá del "cloud" de papel: lecciones del apagón coreano y cómo diseñar infraestructuras verdaderamente resilientes

Madrid, 9 de octubre de 2025 – El reciente incendio en el centro de datos gubernamental de Corea del Sur, que destruyó permanentemente los archivos de 750.000 funcionarios públicos, ha puesto de manifiesto una realidad incómoda: **no todo lo que se llama "nube" lo es realmente**. El incidente, que afectó al G-Drive gubernamental y a 96 sistemas críticos, ilustra los riesgos de confiar en arquitecturas centralizadas sin redundancia geográfica ni copias de seguridad externas, como la del NIRS (National Information Resources Service) en la ciudad de Daejeon en Corea del Sur.

Cuando la "nube" cabe en un edificio

"Lo ocurrido en Corea no es un problema de cloud, sino de diseño", explica **David Carrero, cofundador de Stackscale**, empresa europea especializada en infraestructura cloud privado y bare-metal. "Una nube real no es un único centro de datos con mucho almacenamiento; es redundancia geográfica, automatización de réplicas y recuperación ante desastres. Si un desastre local puede borrar tu servicio, no has construido cloud, has construido un punto único de fallo".

El caso coreano reveló fallos críticos en su diseño: un almacenamiento monolítico sin réplicas externas, 96 sistemas críticos bajo el mismo dominio de fallo y una dependencia total de una única ubicación física. **El resultado: pérdida permanente de datos y miles de horas de productividad volatilizadas.**

De la regla 3-2-1 a la 3-2-1-1-0: evolución necesaria

La estrategia tradicional de copias de seguridad, conocida como regla 3-2-1 (tres copias, dos medios, una fuera de sitio), ha demostrado ser insuficiente ante amenazas modernas como el ransomware o los fallos de proveedores. La evolución hacia la **regla 3-2-1-1-0** añade capas críticas de protección:

- **3** copias de los datos críticos
- **2** tipos diferentes de medios
- **1** copia fuera del sitio principal
- **1** copia offline o air-gapped (desconectada de red)
- **0** errores verificados mediante pruebas regulares

Esta metodología reconoce que los riesgos actuales van más allá de los fallos de hardware. Los ataques de ransomware han evolucionado para cifrar no solo los datos de producción, sino también las copias de seguridad conectadas a la red, mientras que incluso gigantes tecnológicos han protagonizado casos de pérdida permanente de datos por errores administrativos.

Arquitecturas activo-activo: producción que sobrevive al desastre

"La mejor póliza no es una, son varias", señala Carrero. "Producción activo-activo en dos centros de datos distintos y, además, copias inmutables en un tercer emplazamiento. Así, si un sitio cae, conmutas; y si todo va mal, restauras de una copia que no ha podido ser alterada".

Las soluciones con **georeplicación síncrona** permiten desplegar entornos de misión crítica con RPO=0 (sin pérdida de datos) y RTO=0 (sin tiempo de inactividad). Estos sistemas replican datos en tiempo real entre centros de datos separados geográficamente, garantizando que la información permanezca accesible incluso ante desastres que afecten a una ubicación completa.

La **diferencia entre activo-activo y activo-pasivo radica en el tiempo de** respuesta: el primero reparte carga y sobrevive al fallo de forma inmediata, mientras que el segundo requiere conmutación pero ofrece una alternativa más económica cuando un breve downtime es aceptable.

El tercer pilar: backups inmutables en ubicación independiente

Más allá de la producción redundante, la estrategia completa requiere un tercer elemento: **copias de seguridad en un dominio de fallo independiente**, utilizando tecnologías WORM (Write Once, Read Many) o air-gap que impidan su modificación o cifrado por ransomware.

"En Stackscale desplegamos entornos activo-activo o activo-pasivo geo-redundantes, y los complementamos con copias en otro centro de datos", explica Carrero. "Para backup inmutable trabajamos con herramientas como Proxmox Backup Server o Veeam, que permiten retención WORM, verificaciones de restauración y alertas de comportamiento anómalo. La clave no es el software, es el diseño y probar las recuperaciones: sin test, no hay plan de recuperación ante desastres".

Alternativas open source: democratizando la resiliencia

Proxmox Backup Server representa una alternativa open source de nivel empresarial a soluciones propietarias como Veeam o Nakivo. Basado en Debian y desarrollado completamente en Rust para maximizar rendimiento y eficiencia de memoria, ofrece características críticas como:

- Backups incrementales con deduplicación automática
- Compresión ultra rápida con Zstandard
- Soporte para Secure Boot
- Sincronización entre almacenes locales y remotos
- Recuperación granular rápida de VMs, contenedores o archivos individuales
- Integración nativa con Proxmox VE y compatibilidad con VMware, Hyper-V, Kubernetes y otras plataformas

Su modelo de licencia AGPL v3 permite a organizaciones de cualquier tamaño implementar estrategias robustas de backup sin costes de licenciamiento, mientras que el soporte empresarial por suscripción ofrece tranquilidad adicional para entornos de producción críticos.

Lista de verificación: cómo evitar repetir Daejeon

Las organizaciones pueden evaluar su resiliencia mediante estos criterios mínimos:

1. **Dos ubicaciones mínimas** para producción (activo-activo o conmutación probada)
2. **Backups en tercer emplazamiento**, inmutables mediante WORM o air-gap
3. **RPO y RTO definidos** por servicio y ensayados regularmente
4. **Restauraciones probadas** trimestral o semestralmente, no solo logs de "backup OK"
5. **Segregación de credenciales** de backup con autenticación multifactor
6. **Monitorización de anomalías**: borrados masivos, cifrados, cambios de políticas
7. **Cumplimiento normativo**: ENS/ISO 27001 con evidencias de auditoría
8. **Control sobre SaaS**: capacidad de exportación, retención e independencia del proveedor

Conclusión: disciplina frente a glamour

El caso coreano recuerda una verdad fundamental: **la infraestructura resiliente no se construye con marketing sino con disciplina de ingeniería**. Redundancia geográfica real, copias externas inmutables y pruebas periódicas de recuperación son los únicos elementos que evitan que un desastre físico se convierta en una catástrofe digital permanente.

"No es glamour, es disciplina", concluye Carrero. "Y es lo único que evita que, cuando arde un datacenter o simplemente falle, se queme también nuestra memoria digital".

Sobre Stackscale

Stackscale -- https://www.stackscale.com/ -- es una empresa europea del Grupo Aire especializada en infraestructura cloud privado y bare-metal, con más de 8 centros de datos con ubicaciones principales en Madrid y Ámsterdam. Ofrece soluciones de almacenamiento con georeplicación síncrona, cloud privado con Proxmox VE o Vmware, servidores dedicados de alto rendimiento y servicios gestionados para empresas que requieren control total sobre su infraestructura TI sin renunciar a la resiliencia del cloud público.

Contacto de prensa:
Departamento de Marketing de Stackscale : marketing@stackscale.com – T: 911091090