Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

GRAN INTERRUPCIÓN AFECTA A LOS GIGANTES DE LA NUBE AWS Y AZURE

29/10/2025

CONTENIDO

INTRODUCCIÓN

Graves incidentes recientes han impactado el funcionamiento de las plataformas de nube de Amazon Web Services (AWS) y Microsoft Azure, generando interrupciones en servicios globales y reforzando la necesidad de resiliencia multirregional.

GRAN INTERRUPCIÓN AFECTA A LOS GIGANTES DE LA NUBE AWS Y AZURE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_10_29_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	29/10/2025
Es día cero (0 day):	No

RESUMEN

Graves incidentes recientes han impactado el funcionamiento de las plataformas de nube de Amazon Web Services (AWS) y Microsoft Azure, generando interrupciones en servicios globales y reforzando la necesidad de resiliencia multirregional.

Fallos Críticos en la Nube: Azure y AWS

Ambas plataformas experimentaron fallos masivos en sus sistemas centrales de enrutamiento y nombres de dominio.

Azure (29 de octubre de 2025)

- Afectación: Miles de usuarios reportaron fallos en el portal de Azure y servicios vinculados como Microsoft 365.
- Causa probable: Microsoft confirmó que el origen estaba ligado a un fallo del sistema de nombres de dominio (DNS) y/o un problema con Azure Front Door (AFD), el componente que gestiona el enrutamiento de tráfico global. Este fallo impidió que los nombres de servicios se tradujeran correctamente.
- Estado: Microsoft confirma estar investigando activamente el incidente.

AWS (20 de octubre de 2025)

- Afectación: La región más impactada fue US-EAST-1 (Virginia, EE. UU.), la zona de datos más grande y utilizada por AWS. El incidente afectó a al menos 141 servicios diferentes.
- Causa: Un fallo en el sistema de supervisión de balanceadores de carga interna y/o en el sistema de DNS desencadenó una cascada de problemas que paralizó servicios de plataformas ampliamente reconocidas (aplicaciones, juegos, servicios web).

Implicaciones Críticas para la Resiliencia

Estos incidentes demuestran que, incluso los “gigantes” de la nube, dependen de infraestructuras con puntos frágiles (como DNS y enrutamiento), y refuerzan la necesidad de planos de contingencia.

- Dependencia Crítica: El efecto no se limita a las nubes; una empresa que tiene todos sus servicios alojados en una sola región sin respaldo sufre la paralización total de sus operaciones.
- Puntos Frágiles: Los fallos de DNS o de enrutamiento son fallas de infraestructura de nivel base que pueden generar interrupciones globales, a pesar de las redundancias de los proveedores.
- Transparencia y Recuperación: Los tiempos de recuperación pueden ser largos. Es crucial que los proveedores ofrezcan información clara sobre la causa raíz para que los clientes puedan ajustar sus modelos de riesgo.

RECOMENDACIONES

1. Replicación Multi-Región: Verifica en qué región están alojados tus servicios. Si todo está en US-EAST-1 o en una sola zona de disponibilidad, considere replicar la infraestructura en otra región menos dependiente o geográficamente separada.
2. Acceso alternativo y conmutación por error: asegúrese de tener accesos alternativos (vía CLI/API) si el portal de administración (Azure Portal, AWS Console) está inaccesible. Diez procedimientos definidos de conmutación por error (cambio automático al respaldo) o múltiples zonas/regiones de servicio.
3. Auditoría de Recursos: Comprueba si tu proveedor activó algún límite (throttling) para nuevos lanzamientos de instancias o recursos. Esto suele ocurrir tras fallos graves y puede impedir recuperaciones de emergencia.
4. SLAs y Comunicación: Evalúa los contratos de servicio (SLAs) y el impacto económico de una interrupción prolongada. El equipo de TI debe estar preparado para comunicar interna y externamente la situación con claridad.

NOTICIA COMPLETA

https://devel.group/blog/gran-interrupcion-afecta-a-los-gigantes-de-la-nube-aws-y-azure/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group