Alerta

Técnica

Falla Global en Microsoft Azure

COLCERT AL-20251030 - 081

TLP:CLEAR

Durante la jornada del miércoles, 29 de octubre de 2025, **Microsoft confirmó una interrupción global en su plataforma en la nube Azure**, específicamente relacionada con el servicio Azure Front Door (AFD), responsable de gestionar la distribución global de tráfico web y la entrega de contenidos a través de múltiples de servicios y aplicaciones en línea.

La falla comenzó aproximadamente a las 11:00 a.m. (hora Colombia) y generó problemas de conectividad, lentitud, errores de autenticación y caídas parciales en múltiples servicios dependientes de la infraestructura de Azure. El impacto fue reportado principalmente en regiones de América, Europa y Asia.

Servicios y plataformas afectadas

De acuerdo con la información pública disponible, la falla impactó tanto a servicios propios de Microsoft como a plataformas de terceros que utilizan su infraestructura. Entre los servicios reportados con fallas se encuentran:

- **Azure Portal**, **Azure Active Directory** y **Azure Front Door**.
- **Microsoft 365** (Outlook, Teams, OneDrive, SharePoint).
- **La plataforma Xbox Live** y **Microsoft Store**.
- Sitios web corporativos, portales bancarios y otros servicios digitales que dependen de Azure para autenticación, balanceo de carga o alojamiento.

En algunos países de América Latina, **entidades financieras**, **comercios electrónicos** y **plataformas de servicios en línea** también registraron intermitencias o interrupciones derivadas del problema.

Causa preliminar

Microsoft informó que la afectación se originó en **Azure Front Door**, una red global de distribución de contenido (CDN, por sus siglas en Ingles), encargada de enrutar y optimiza el tráfico web hacia los servicios hospedados en la nube. Un error en esta capa provocó fallas en la conectividad y en la resolución de dominios asociados a servicios de **Azure**, generando tiempos de espera prolongados y errores HTTP para los usuarios finales.

Acciones y mitigación por parte de Microsoft

Microsoft confirmó haber implementado medidas temporales de contención, incluyendo el desvío de tráfico y bloqueo de cambios de configuración mientras se estabiliza la red. Se recomienda a los administradores de sistemas **usar herramientas alternativas** como **Azure CLI** o **PowerShell** en caso de no poder acceder al portal principal. Los servicios comienzan a mostrar mejoras graduales, aunque Microsoft no ha publicado una hora estimada de resolución completa.

Riesgos de ciberseguridad asociados (ataques de oportunidad)

Durante grandes interrupciones o fallas en servicios ampliamente utilizados como Microsoft Azure, los actores maliciosos suelen aprovechar la confusión y el aumento de las búsquedas de información oficial para ejecutar ataques de oportunidad. Entre los principales riesgos se encuentran:

- **Suplantación de comunicaciones oficiales**: envío de correos, mensajes o publicaciones falsas que aparentan provenir de Microsoft o de los equipos de soporte, con el fin de obtener credenciales o información confidencial.
- **Difusión de sitios fraudulentos**: creación de páginas que simulan ser paneles de estado o portales de soporte técnico de Azure para captar datos de acceso de empresas o usuarios.
- **Ataques de *phishing* (correos electrónicos) y *smishing (mensajes SMS)*** : uso de mensajes con supuestos enlaces de recuperación de servicios o verificación de cuentas para distribuir archivos maliciosos o redirigir a portales falsos.
- **Ingeniería social**: intentos de engañar a personal técnico o administrativo aprovechando la urgencia por restablecer servicios o validar configuraciones en la nube.

Recomendaciones generales

Para ciudadanos y usuarios

- Si experimenta lentitud o imposibilidad de acceder a servicios como Outlook, Teams o OneDrive, no realizar cambios de configuración ni elimine cuentas; el problema es de origen global.
- Esperar a la confirmación oficial de restablecimiento desde los canales de Microsoft.
- Mantener precaución frente a posibles intentos de suplantación o fraude. Los atacantes pueden aprovechar la situación para enviar correos o mensajes falsos haciéndose pasar por Microsoft o por áreas de soporte técnico.

Para administradores y equipos técnicos

- Monitorear los servicios alojados o autenticados mediante Azure.
- Evitar realizar despliegues, cambios de DNS o configuraciones críticas durante la afectación, ya que podrían generar inconsistencias o fallos no detectados una vez que el proveedor restablezca el servicio.
- Mantener comunicación con los usuarios internos para mitigar confusión o acciones no autorizadas.
- Documentar el incidente en el plan de continuidad y resiliencia tecnológica, considerando dependencias con proveedores de nube.
- Documentar el incidente detalladamente en los planes de continuidad del negocio (BCP) y resiliencia tecnológica, incluyendo métricas de impacto, tiempos de recuperación (RTO/RPO), y comunicaciones con el proveedor

Fuentes

Reuters, 29 octubre 2025, Microsoft Azure, 365 outage impacting businesses globally starting to ease, noticia.
https://www.reuters.com/technology/microsoft-azure-down-thousands-users-downdetector-shows-2025-10-29/

Infobae, 29 octubre 2025, Falla global de Microsoft Azure: un 'miércoles negro' con fallas en internet, noticia.
https://www.infobae.com/tecno/2025/10/29/falla-global-de-microsoft-azure-un-miercoles-negro-con-fallas-en-internet/

Microsoft 365 Status (X), 29 octubre 2025, Investigating reports of issues accessing Microsoft 365 services and the Microsoft 365 admin centre (tuit oficial), red social.
https://x.com/MSFT365Status/status/1983584467664212431

Microsoft Azure Status, 29 octubre 2025, Azure Front Door – Connectivity issues – Observing recovery, página de estado.
https://azure.status.microsoft/en-us/status

The Verge, 29 octubre 2025, A massive Microsoft Azure outage is taking down Xbox and 365, noticia.
https://www.theverge.com/news/809142/microsoft-azure-xbox-365-is-down-outage