Alerta ID:	0027
Fecha del reporte:	11/09/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Autenticación Multifactor (MFA) Obligatoria – Fase 2
Herramienta de detección	Sitio oficial de Microsoft
Activo involucrado:	Azure Resource Manager, CLI, PowerShell, Mobile App, SDKs, REST API
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la implementación obligatoria de autenticación multifactor (MFA) en Azure a partir del 1 de octubre de 2025 en su Fase 2, que exigirá MFA para cualquier operación de gestión de recursos (crear, actualizar o eliminar) realizada a través de herramientas como Azure CLI, PowerShell, portal móvil, API REST, SDKs o infraestructuras como código (IaC). El propósito es promover una rápida adopción para proteger los entornos de gestión de recursos frente a accesos no autorizados.

Riesgo:

Si no se habilita MFA, los usuarios y scripts podrían quedar vulnerables a compromisos de cuentas, accesos no autorizados o manipulaciones maliciosas en los recursos del entorno. Esta medida se orienta a evitar precisamente este tipo de explotación, ya que se considera una de las defensas más eficaces contra ataques de usurpación de identidad.

Detalle de la fase 2 – Aplicaciones Afectadas

- **Inicio:** 1 de octubre de 2025 (implementación gradual mediante Azure Policy)
- **Aplicaciones / Clientes afectados:**
  - Azure CLI (vía Azure Resource Manager)
  - Azure PowerShell
  - Azure Mobile App
  - SDKs (como Azure SDK e IaC tools)
  - REST API (Control Plane)

Excluidos: Operaciones de solo lectura no requerirán MFA.
Identidades no impactadas: Workload identities como managed identities o service principals.

Recomendaciones de actualización:

- Habilitar MFA para todos los usuarios que realicen operaciones de gestión en Azure antes del 1 de octubre de 2025.
- Aplicar políticas mediante Azure Policy en modo auditoría o cumplimiento para evaluar el impacto y prepararse gradualmente.
- Actualizar herramientas a las versiones recomendadas:
  - Azure CLI ≥ 2.76
  - Azure PowerShell ≥ 14.3
  - Migrar cuentas usadas como servicio (user-based service accounts) a workload identities (managed identities o service principals).
  - Postergar la obligatoriedad, en caso necesario, hasta el 1 de julio de 2026, gestionado por un Administrador Global desde el portal de Azure.

Pasos para la actualización:

1. Identificar qué usuarios necesitan MFA configurado.
2. Aplicar una política integrada de Azure Policy para bloquear operaciones si MFA no está presente.
3. Verificar y actualizar las herramientas (CLI 2.76+, PowerShell 14.3+).
4. Migrar las identidades basadas en usuario a identidades de trabajo (workload identities)

Fuentes:

- https://azure.microsoft.com/en-us/blog/azure-mandatory-multifactor-authentication-phase-2-starting-in-october-2025/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.