

## Mala práctica de seguridad detectada en Azure Active Directory

COLCERT AL-20250904-074

TLP: CLEAR

Se ha identificado la exposición de credenciales de **Azure Active Directory**, como **ClientId** y **ClientSecret** en archivos de configuración accesibles públicamente, lo que representa una exposición de secretos de aplicación (client secret/certificado) con alta probabilidad de ser aprovechada por actores maliciosos. Esta situación no solo habilita el acceso no autorizado mediante **Microsoft Graph** y otros servicios en la nube, sino que abre la puerta a movimientos laterales, escalamiento de privilegios y posibles compromisos masivos de datos corporativos.



Azure Active Directory

De mantenerse esta práctica, es probable que se incremente la frecuencia y sofisticación de los ataques contra entornos híbridos y *cloud*, lo que podría derivar en incidentes con un impacto operativo, financiero y reputacional significativo. Aunque el nivel de incertidumbre está presente, el riesgo es alto y requiere decisiones estratégicas inmediatas para reforzar el manejo de secretos, aplicar controles preventivos como MFA y fortalecer la detección temprana de accesos anómalos.

**Activos afectados**

Los activos directamente expuestos son **Azure AD** y las aplicaciones registradas, pero el efecto cascada puede impactar en todo el ecosistema de **Microsoft 365** y los servicios en la nube conectados, escalando el incidente a nivel organizacional.

La lista de activos vulnerables afectados por esta vulnerabilidad de filtración de Client Secrets en Azure Active Directory, junto con su función principal:

- ❑ **ClientId y ClientSecret de la aplicación Azure AD:** identifican y autentican una aplicación confiable en Azure AD. El ClientSecret actúa como una contraseña para que la app pueda obtener tokens OAuth 2.0.
- ❑ **Aplicaciones registradas en Azure AD:** son las que usan estas credenciales para autenticar y acceder a recursos Microsoft 365 y Azure.
- ❑ **Microsoft Graph API:** interfaz que permite acceder a datos y servicios de Microsoft 365 (usuarios, grupos, mails, archivos, roles).
- ❑ **Usuarios y grupos del tenant Azure AD:** actores organizacionales identificados dentro del directorio; la enumeración permite a atacantes identificar objetivos valiosos.
- ❑ **Recursos compartidos de Microsoft 365 (SharePoint, OneDrive, Exchange Online):** servicios donde se almacenan datos sensibles accesibles a través de permisos concedidos a aplicaciones.
- ❑ **Aplicaciones maliciosas desplegadas bajo el tenant:** activos que atacantes pueden registrar para mantener persistencia y escalar privilegios dentro del entorno.
- ❑ **Archivos de configuración appsettings.json u otros similares:** contienen secretos y configuración crítica para la autenticación y autorizaciones de la aplicación.

NIVEL DE RIESGO

**ALTO**

## ¿Cómo se materializa este riesgo?

No es un fallo en Azure AD en sí, sino una mala práctica de gestión de la seguridad: la exposición pública de archivos de configuración (por ejemplo, appsettings.json) que contienen secretos como ClientId y ClientSecret. Un ciberdelincuente puede explotar esta situación de la siguiente manera:

- Búsqueda de archivos expuestos:** los ciberdelincuentes rastrean repositorios públicos (GitHub, GitLab, Bitbucket) o servidores mal configurados en Internet para localizar archivos como appsettings.json, .env, .config, etc. Estos archivos suelen contener credenciales de aplicaciones registradas en Azure AD.
- Extracción de credenciales:** el atacante identifica valores como
  - **TenantId** (identificador de la organización en Azure – no es secreto).
  - **ClientId** (identificador de la aplicación registrada - Público).
  - **ClientSecret** (clave privada de la aplicación - Secreto).
- Autenticación mediante OAuth 2.0 (Client Credentials Flow):** con ClientId y ClientSecret, el atacante solicita un token de acceso directamente al endpoint de Azure AD (<https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token>). El MFA no aplica a este flujo (debido a que no hay interacción del usuario). Azure AD, al recibir credenciales válidas, entrega un JWT token que otorga acceso con los permisos asignados a la aplicación, esto ya que el token hereda todos los permisos ya consentidos para la aplicación.
- Acceso a Microsoft Graph API u otros servicios:** con el token, el atacante puede interactuar con Microsoft Graph API u otros recursos autorizados. El impacto depende de los permisos de API/Graph concedidos a la aplicación y del consentimiento del administrador
- Escalamiento de privilegios y persistencia:** si la aplicación tenía permisos elevados (por ejemplo, Directory.ReadWrite.All o Mail.ReadWrite), el actor de amenaza puede modificar directorios, crear nuevas aplicaciones maliciosas o incluso otorgarse más privilegios. Esto le permite mantener acceso a largo plazo e incluso moverse lateralmente hacia otros recursos.



## IMPACTO PARA COLOMBIA Y LA REGIÓN

La exposición de ClientId y ClientSecret en **Azure AD** plantea un riesgo estratégico para Colombia y Latinoamérica, donde muchas organizaciones públicas y privadas ya migraron o están en proceso de migración hacia Microsoft 365 y Azure.

- ❑ **Aumento del riesgo de ciberespionaje y captura de información sensible:** entidades del sector gubernamental, financiero, salud y telecomunicaciones que usan Azure AD quedan en riesgo de que actores de amenaza obtengan acceso a correos, documentos, historiales médicos o datos de clientes.
- ❑ **Posibilidad de ataques de ransomware más avanzados:** los grupos que operan en la región pueden aprovechar accesos a SharePoint, Exchange o Teams para distribuir cargas maliciosas o cifrar información a gran escala.
- ❑ **Impacto en la continuidad de servicios críticos:** muchas entidades colombianas y latinoamericanas utilizan Azure para gestionar servicios en energía, transporte, salud y sector público. Un compromiso de identidades podría derivar en interrupciones de operaciones esenciales. En la región, donde la resiliencia digital aún es desigual, el impacto de una caída puede ser mayor y más prolongado.
- ❑ **Incremento en fraudes y ataques a usuarios finales:** con acceso a correos y sistemas internos, los atacantes pueden realizar ingeniería social avanzada. Esto se conecta con el auge del cibercrimen organizado en Latinoamérica, donde bandas locales aprovechan accesos iniciales vendidos en foros clandestinos.
- ❑ **Debilitamiento de la confianza digital y reputación:** un ataque exitoso afectaría la confianza en la transformación digital de las organizaciones colombianas, especialmente en sectores donde la adopción de nube es aún vista con cautela. Esto puede frenar proyectos estratégicos de digitalización y generar un efecto dominó en la región.

## Técnicas MITRE ATT&CK Asociadas

Estas son las principales técnicas MITRE ATT&ACK asociadas a la explotación de la vulnerabilidad en Azure AD.

TÉCNICA	CÓDIGO	DESCRIPCIÓN
<b>Obtención de credenciales en repositorios de código</b>	T1552.001	Los adversarios buscan credenciales almacenadas de forma insegura en archivos de configuración (appsettings.json, .env, .config) o repositorios públicos. Estas credenciales permiten autenticarse en servicios cloud como Azure AD.
<b>Uso de credenciales válidas</b>	T1078	Una vez obtenidos ClientId y ClientSecret, el atacante puede autenticarse legítimamente contra Azure AD mediante OAuth 2.0. Esto les permite operar como una aplicación confiable, evadiendo controles tradicionales de seguridad.
<b>Acceso a API de servicios en la nube</b>	T1526	Tras autenticarse, el adversario utiliza Microsoft Graph API y otros servicios en la nube para descubrir usuarios, grupos, roles y recursos disponibles. Este reconocimiento es clave para movimientos posteriores, como escalamiento de privilegios o exfiltración de datos.
<b>Robo/uso de tokens de acceso a la aplicación</b>	T1528	Esta se centra en el robo o reaprovechamiento de tokens de acceso (por ejemplo, OAuth, JWT) ya emitidos a una aplicación o servicio. Con ellos, un atacante puede asumir identidades válidas, ejecutar acciones en nombre de un usuario e integrarse a aplicaciones cloud sin autenticación.
<b>Uso de material alternativo de autenticación: Tokens de aplicación</b>	T1550.001	Los atacantes emplean tokens de aplicaciones móviles o de escritorio como un medio alternativo para autenticarse en servicios, sin la necesidad de credenciales de usuario (usuario/contraseña). Esto les permite evadir controles de MFA y acceder a recursos directamente, aprovechando tokens previamente emitidos o robados.
<b>Descubrimiento de cuentas y permisos vía Graph</b>	T1087 / T1069	1) El atacante enumera usuarios, grupos o roles disponibles en el entorno. 2) Se inspeccionan privilegios asociados a cuentas, grupos o roles para identificar permisos excesivos o rutas de escalamiento de privilegios. 3) Usualmente se realiza mediante APIs como Microsoft Graph o similares en entornos cloud.
<b>Manipulación de permisos/roles en nube</b>	T1098.003/004	Los atacantes, tras comprometer credenciales o una cuenta en la nube, modifican roles, permisos o políticas para escalar privilegios o mantener acceso. 003: Cambiar roles de IAM para conceder privilegios administrativos. 004: Ajustar políticas de asignación de roles (Role Assignment) para dar acceso persistente a cuentas controladas.
<b>Creación de servicio principal para persistencia</b>	T1136.003	El adversario crea un nuevo Service Principal (identidad de aplicación) en un entorno cloud. Esto les permite mantener persistencia, autenticarse en servicios y operar con permisos otorgados, incluso si las credenciales iniciales se revocan.

## Mitigaciones MITRE

Estas son las principales mitigaciones recomendadas por MITRE ATT&ACK para contrarrestar la explotación de la vulnerabilidad identificada.

MITIGACIÓN	CÓDIGO	RELEVANCIA
Gestión de credenciales	M1027	Establecer políticas de gestión de credenciales seguras (no incrustarlas en archivos de configuración, uso de gestores como Azure Key Vault, rotación periódica de secretos). Esto ataca directamente la raíz del problema: la exposición de ClientSecret.
MFA (Autenticación multifactor)	M1032	Aunque se expongan credenciales, exigir MFA en accesos críticos reduce drásticamente la posibilidad de que un atacante las use sin un segundo factor. Relevante para servicios y cuentas privilegiadas asociadas a Azure AD.
Principio de privilegio mínimo	M1018	Limitar los permisos que tienen las aplicaciones registradas en Azure AD (ej. evitar Directory.ReadWrite.All si no es necesario). Si un ClientSecret se ve comprometido, el impacto será mucho menor.

## Conclusiones








- ❑ La exposición de Client Secrets en archivos de configuración públicos permite a ciberdelincuentes autenticarse como aplicaciones legítimas sin necesidad de interacción de usuario ni MFA, representando un riesgo alto para la seguridad cloud.
  - ❑ Esta vulnerabilidad posibilita el acceso no autorizado a datos sensibles de Microsoft 365 y Azure, incluyendo usuarios, grupos, correos y archivos, con potenciales consecuencias legales y reputacionales.
  - ❑ Los secretos expuestos pueden ser usados para desplegar aplicaciones maliciosas dentro del tenant, permitiendo persistencia, escalación de privilegios y movimientos laterales dentro del entorno.
- ❑ La falta de gestión segura de secretos y configuración incorrecta de servidores contribuyen significativamente a la ocurrencia de estas filtraciones.
  - ❑ La detección y respuesta rápida a exposiciones de Client Secrets sigue siendo un desafío, lo que aumenta la probabilidad de impacto severo y sostenido en la nube.



NIVEL DE RIESGO

**ALTO**

## Recomendaciones

-  No almacenar Client Secrets directamente en archivos de configuración accesibles públicamente; utilizar herramientas especializadas como Azure Key Vault para gestión segura y centralizada de secretos.
-  Configurar los servidores para negar acceso a archivos sensibles (.json, .config) mediante reglas estrictas en IIS, Nginx o Apache que bloqueen la exposición pública.
-  Implementar la rotación automática frecuente de Client Secrets y certificados para minimizar el tiempo de validez de posibles credenciales expuestas.
-  Aplicar el principio de menor privilegio a las aplicaciones registradas, limitando los permisos a solo lo estrictamente necesario para su funcionamiento.
-  Habilitar monitoreo, alerta y auditoría en Azure AD para detectar accesos inusuales o uso de aplicaciones con Client Secrets, apoyándose en logs y servicios como Azure Monitor y Defender for Cloud.

## Fuentes

- Resecurity, 30 de agosto de 2025, 3 de septiembre de 2025, Azure AD Client Secret Leak: The Keys to Cloud, Fuente especializada en ciberseguridad.**  
 <https://www.resecurity.com/blog/article/azure-ad-client-secret-leak-the-keys-to-cloud>
- Cyber Security News, 2 de septiembre de 2025, 3 de septiembre de 2025, Azure Active Directory Vulnerability Exposes Credentials in Public Files, Medio digital de noticias en ciberseguridad.**  
 <https://cybersecuritynews.com/azure-active-directory-vulnerability/>