ESQUEMA EXACTO: ROLES EN AZURE (CONTRASTADO CON DOCUMENTACIÓN OFICIAL DE MICROSOFT)

CAPA 1: Microsoft Entra ID (anteriormente Azure AD)

¿Qué gestiona? Identidades del tenant (usuarios, grupos, aplicaciones, políticas de acceso).

Ámbito: Tenant-wide (nivel de directorio).

NO da acceso directo a recursos de Azure (VMs, Storage, etc.) *a menos que se le asigne RBAC*.

ROL	¿QUÉ PUEDE HACER?	¿QUÉ NO PUEDE HACER?	RIESGO REAL
GLOBAL ADMINISTRATOR	• Gestionar TODO en Entra ID • Asignar CUALQUIER rol de Entra ID • Configurar políticas de seguridad/MFA • Elevar acceso para obtener `User Access Administrator` en RBAC a nivel raíz (/) [[94]]	• NO tiene acceso automático a recursos de Azure (RBAC) • Para acceder a recursos, debe autoasignarse un rol RBAC	⚠️ MÁXIMO (puede escalar a control total de recursos mediante "elevate access")
PRIVILEGED ROLE ADMINISTRATOR	• Gestionar asignaciones de roles en Entra ID • Asignar `Global Administrator` a otros usuarios (y a sí mismo) [[106]] [[108]]	• NO puede gestionar recursos de Azure directamente • Requiere permisos adicionales para acceder a recursos	⚠️ MÁXIMO (puerta trasera a `Global Administrator`)
USER ADMINISTRATOR	• Crear/gestionar usuarios y grupos • Resetear contraseñas • Asignar roles NO privilegiados (ej.: Helpdesk Administrator) [[96]]	• NO puede asignar `Global Administrator` ni `Privileged Role Administrator` [[96]] • NO puede modificar políticas de seguridad críticas	⚠️ BAJO-MEDIO (solo gestiona identidades básicas)
SECURITY ADMINISTRATOR	• Ver/configurar políticas de seguridad • Gestionar Conditional Access • Ver auditorías	• NO puede asignar roles de Entra ID • NO puede crear usuarios	⚠️ MEDIO (reconocimiento de vulnerabilidades)

📌 CAPA 2: Azure RBAC (Role-Based Access Control)

¿Qué gestiona? Acceso a recursos de Azure (VMs, Storage, Key Vault, redes).

Ámbito: Jerárquico (Management Group → Suscripción → Resource Group → Recurso).

NO da acceso a Entra ID (a menos que se le asigne un rol de Entra ID).

ROL	¿QUÉ PUEDE HACER?	¿QUÉ NO PUEDE HACER?	RIESGO REAL
OWNER	• Control total sobre recursos en su scope • Asignar CUALQUIER rol RBAC dentro de su scope • Crear/eliminar/modificar recursos	• NO puede asignar roles de Entra ID (ej.: Global Administrator) • Su control está limitado a su scope (ej.: una suscripción)	⚠️ MÁXIMO (dentro de su scope)
USER ACCESS ADMINISTRATOR	• Asignar roles RBAC a otros usuarios • Ver todos los recursos (*/read) • NO puede modificar recursos (solo gestionar acceso) [[116]]	• NO es un rol de Entra ID • NO puede asignar roles de Entra ID (Global Admin, User Admin, etc.) [[120]] • Solo gestiona permisos RBAC	⚠️ ALTO (puede asignarse `Owner` dentro de su scope)

CONTRIBUTOR	• Crear/modificar/eliminar recursos • Acceder a datos (dependiendo del recurso)	• NO puede asignar roles RBAC • NO puede gestionar acceso de otros usuarios	⚠️ MEDIO (puede crear recursos maliciosos o explotar MSI)
READER	• Ver recursos y configuraciones • Listar secretos (pero no acceder a ellos)	• NO puede modificar nada • NO puede asignar roles	⚠️ BAJO (solo reconocimiento)

FRASE CLAVE PARA NO CONFUNDIRSE (OFICIAL DE MICROSOFT)

"Entra ID roles ≠ RBAC roles.

User Administrator (Entra ID) gestiona usuarios.

User Access Administrator (RBAC) gestiona permisos a recursos.

Global Administrator (Entra ID) puede escalar a Owner (RBAC) mediante 'elevate access', pero User Access Administrator (RBAC) NUNCA puede escalar a Global Administrator." [[94]] [[102]]

PERSPECTIVA DE HACKING: VECTORES DE ESCALADA REALES (LEGÍTIMOS PARA AUDITORÍA)

🟤 Vector 1: Global Administrator → Control total (EL MÁS CRÍTICO)

¿Cómo funciona?

1. Un atacante compromete una cuenta con rol `Global Administrator` en Entra ID (ej.: phishing, credenciales filtradas).
2. Usa la función "Elevate access" en Entra ID → Properties [[94]]:
    a. Esto le asigna automáticamente el rol `User Access Administrator` en RBAC a nivel raíz (`/`).
3. Como `User Access Administrator` en RBAC, se autoasigna `Owner` en todas las suscripciones.
4. Resultado: Control total sobre TODOS los recursos de Azure + TODAS las identidades de Entra ID.

¿Por qué es el peor?

- Es la única forma de obtener control absoluto sobre el tenant completo.
- Microsoft recomienda máximo 5 usuarios con este rol [[127]].

🟤 Vector 2: Privileged Role Administrator → Global Administrator

¿Cómo funciona?

1. Un atacante encuentra un usuario con rol `Privileged Role Administrator` en Entra ID (mal asignado).
2. Este rol puede asignar `Global Administrator` a cualquier usuario, incluido a sí mismo [[108]].
3. Una vez con `Global Administrator`, sigue el Vector 1 para controlar recursos.

¿Dónde se encuentra?

- En entornos con PIM (Privileged Identity Management) mal configurado.
- Cuando se delega gestión de roles sin controles adecuados.

🟢 Vector 3: User Access Administrator (RBAC) → Owner (dentro de scope)

¿Cómo funciona?

1. Un atacante compromete una cuenta con rol `User Access Administrator` en RBAC (ej.: en una suscripción específica).
2. Se autoasigna `Owner` dentro del mismo scope (ej.: esa suscripción).
3. Resultado: Control total sobre esa suscripción, pero NO sobre Entra ID ni otras suscripciones.

¿Por qué NO es tan crítico?

- El atacante no puede escalar a Global Administrator (es un rol de Entra ID, no de RBAC).
- Su control está limitado al scope donde tiene `User Access Administrator`.

🟢 Vector 4: Contributor + MSI (Managed Identity) → Lateral Movement

¿Cómo funciona?

1. Un atacante con rol `Contributor` en un Resource Group crea una VM con System Assigned Managed Identity.
2. Si esa MSI tiene acceso a un Key Vault (ej.: por una política mal configurada), el atacante:
    a. Accede al Key Vault desde la VM.
    b. Roba secretos/certificados.
    c. Usa esas credenciales para acceder a otros recursos (ej.: bases de datos, otras suscripciones).

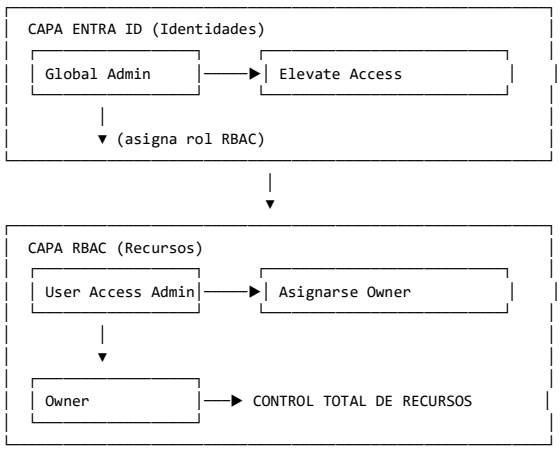
¿Dónde se encuentra?

- Entornos con políticas de acceso a Key Vault demasiado permisivas.
- MSI asignadas a recursos sin principio de mínimo privilegio.

🛡 MEJORES PRÁCTICAS PARA DEFENDERSE (SEGÚN MICROSOFT)

Rol crítico	Recomendación oficial
Global Administrator	• Máximo 5 usuarios [[127]] • Usar PIM para acceso temporal • Revisar auditorías mensualmente
Privileged Role Administrator	• Solo para equipo de seguridad • Nunca asignar permanentemente (solo vía PIM)
User Access Administrator (RBAC)	• Asignar solo al scope mínimo necesario (nunca a nivel raíz /) • Auditar asignaciones mensualmente

Contributor	• Evitar en scope alto (suscripción) • Usar roles más específicos (ej.: Virtual Machine Contributor)



⚠️ NOTA: User Administrator (Entra ID) NO aparece en este flujo
porque NO puede escalar a Global Administrator.

CONCLUSIÓN FINAL

1. El rol más peligroso: `Global Administrator` (Entra ID) + "elevate access" → control total.
2. Confusión común: `User Access Administrator` es RBAC (gestiona recursos), NO Entra ID. Nunca puede asignar Global Administrator.
3. User Administrator es seguro por diseño: Microsoft lo limitó explícitamente para que NO pueda asignar roles críticos [[96]].
4. La escalada real siempre pasa por:
    a. `Privileged Role Administrator` → `Global Administrator` → `Owner` (RBAC), O
    b. `Global Administrator` → "elevate access" → `Owner` (RBAC).