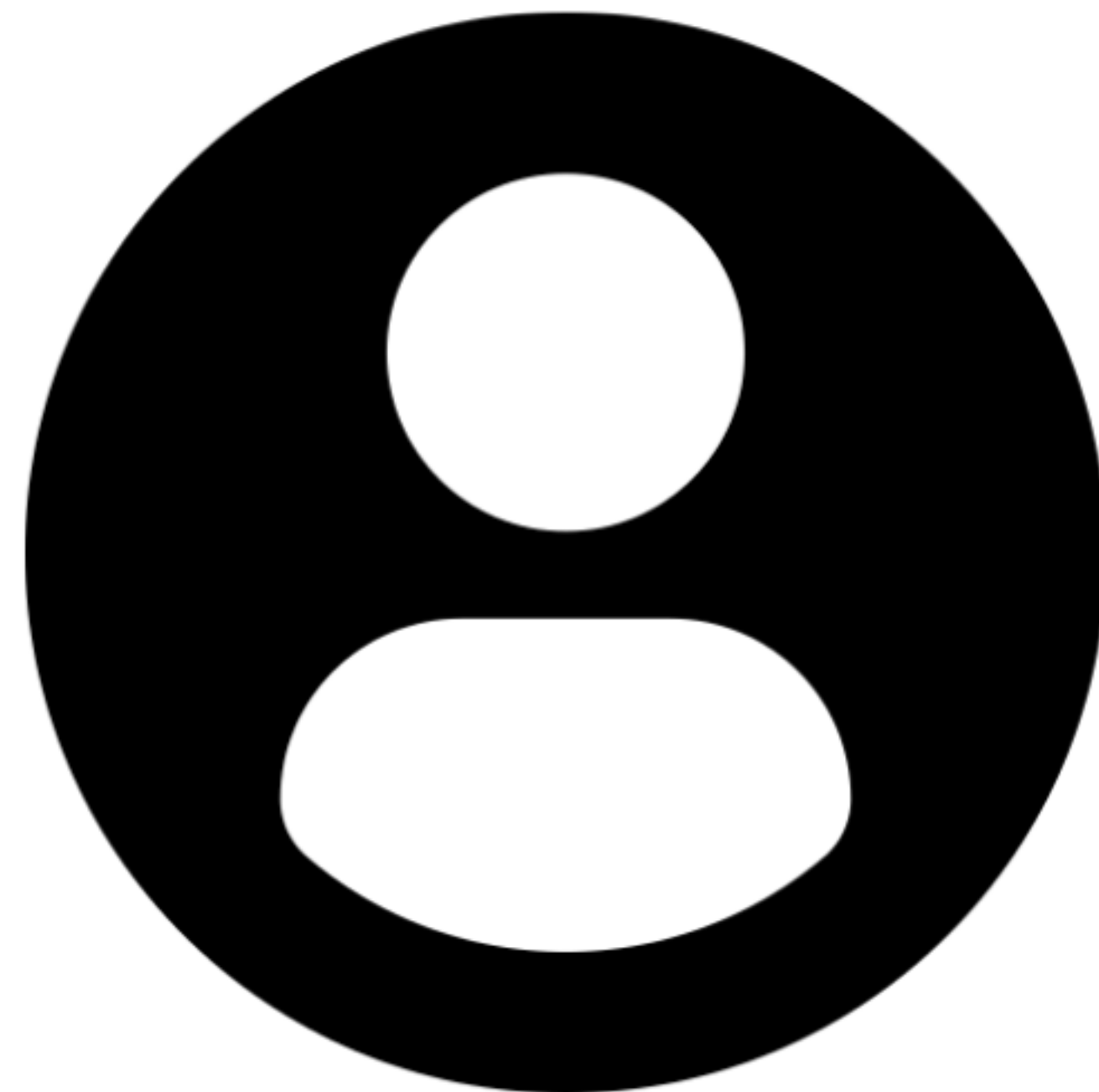




Autenticación y Autorización en Aplicaciones Web

Introducción

- **Autenticación y Autorización** son componentes fundamentales para la seguridad de las aplicaciones web modernas.
- **Objetivo:** Entender las diferencias clave, explorar métodos populares y mejores prácticas, y examinar su implementación en un caso práctico.



Definición y Diferencias Clave

- **Autenticación:** Verificación de la identidad del usuario. Responde a la pregunta: **¿Quién eres?**
- **Autorización:** Determina qué recursos o acciones tiene permitido realizar un usuario autenticado. Responde a la pregunta: **¿Qué puedes hacer?**

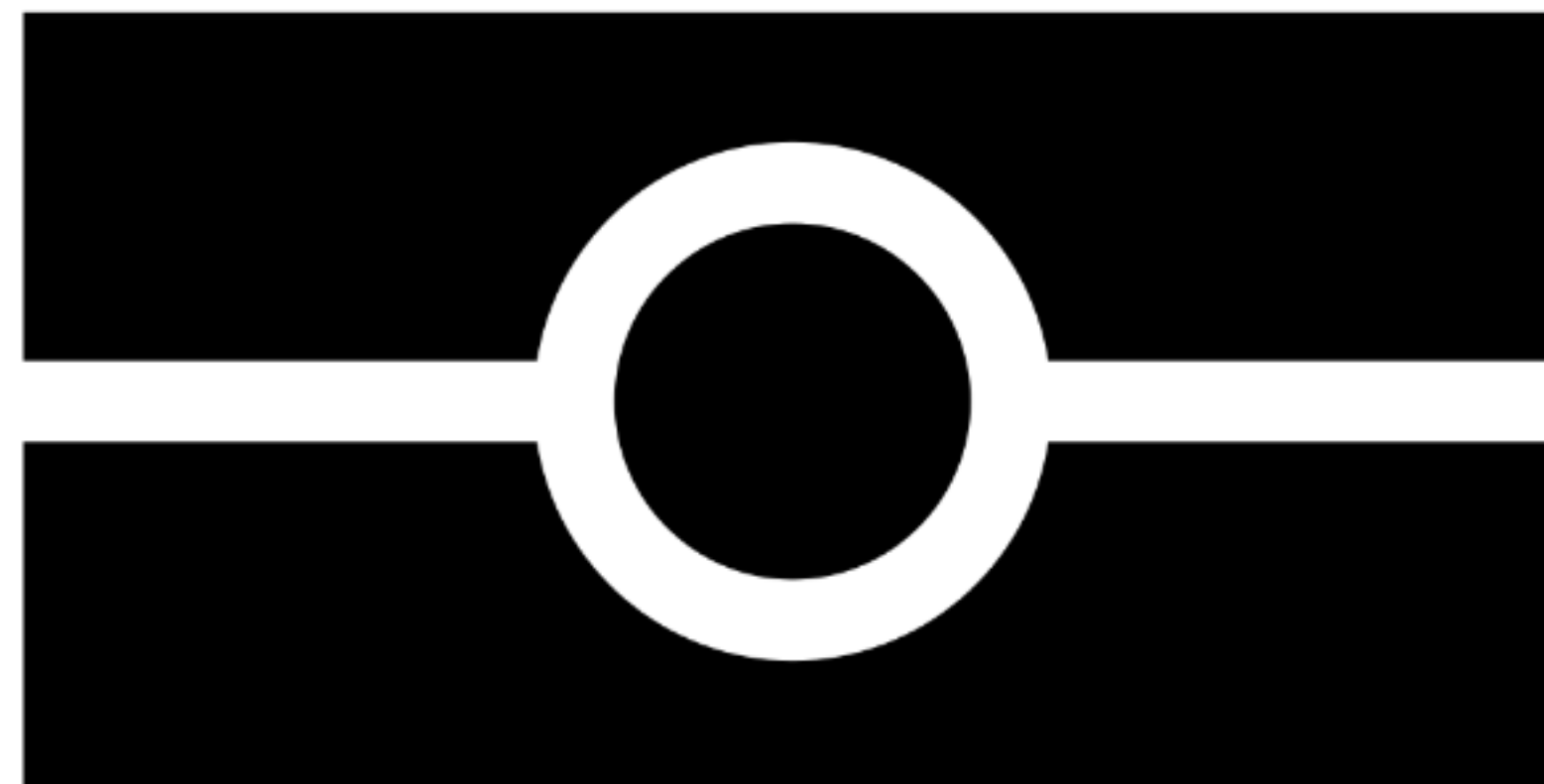
Diferencias Clave:

- **Autenticación** ocurre primero, **autorización** después.
- **Autenticación** verifica la identidad; **autorización** gestiona los privilegios de acceso.



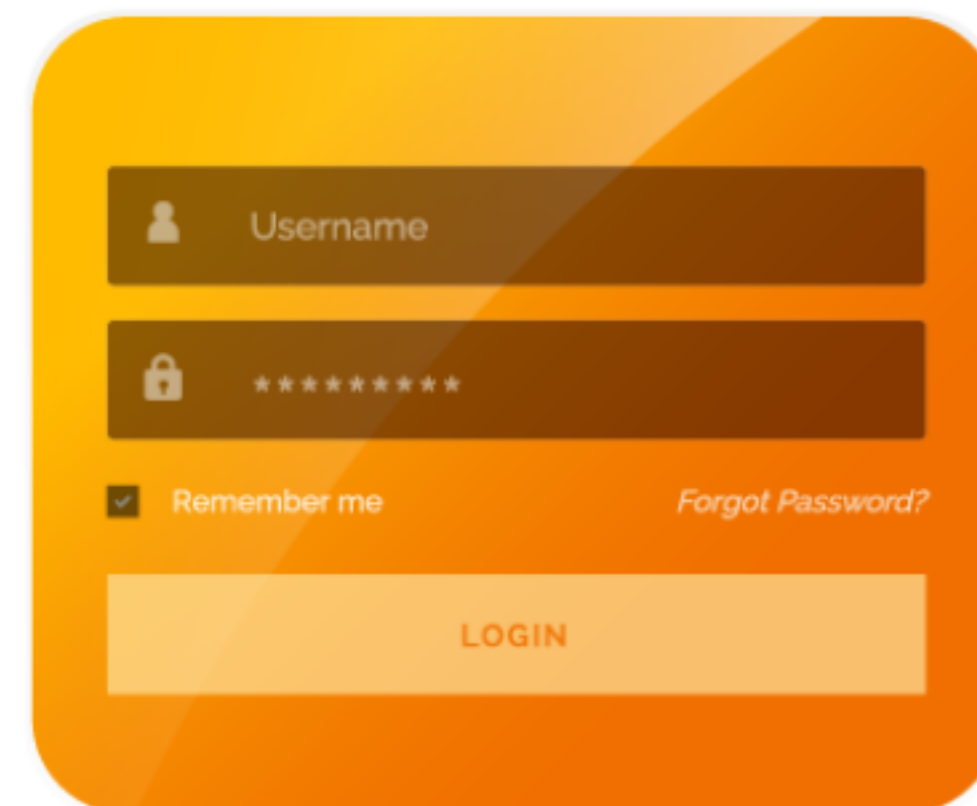
Métodos de Autenticación Más Comunes

- **Contraseñas:** Método más tradicional, con **hashing y salting** para seguridad adicional.
- **Tokens y Estándares Abiertos (JWT, OAuth):**
 - **JWT:** Permite compartir información de identidad de manera segura.
 - **OAuth:** Permite la delegación de accesos a recursos sin compartir credenciales directamente.
- **Autenticación Biométrica:** Uso de características físicas, como huellas dactilares.
- **Autenticación Multifactor (MFA):** Combina múltiples métodos de autenticación para mayor seguridad.



Métodos de Autorización Recomendados

- **RBAC (Role-Based Access Control):**
 - Asigna permisos según el rol del usuario en la organización.
 - Ejemplo: Estudiantes, Profesores, Administradores.
- **ABAC (Attribute-Based Access Control):**
 - Se basa en atributos del usuario y contexto (ubicación, hora, etc.).
- **Control Basado en Reglas:**
 - Define accesos según reglas específicas (horarios, ubicación, dispositivos).



A stylized illustration of a login form on a yellow-to-orange gradient background. The form includes a 'Username' input field with a person icon, a password input field with a lock icon and masked characters, a 'Remember me' checkbox, a 'Forgot Password?' link, and a 'LOGIN' button.

Aplicación Práctica – Caso Educativo

Escenario:

Plataforma educativa en línea con tres tipos de usuarios:

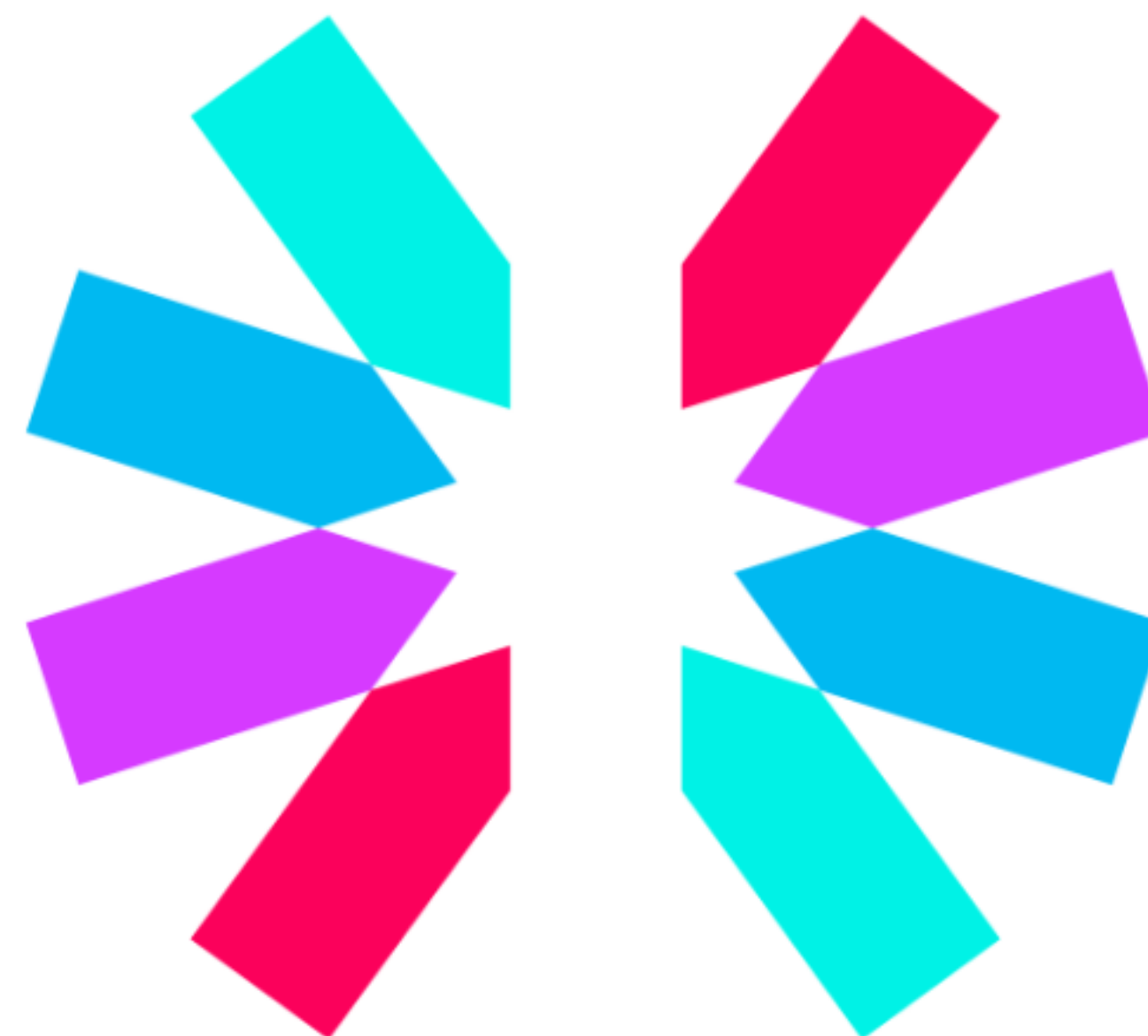
Estudiantes, Profesores y Administradores.

Solución Recomendada:

- **Autenticación MFA** para garantizar identidad (contraseña + token).
- **JWT** para manejar sesiones seguras.
- **RBAC** para gestionar accesos según roles:
 - **Estudiantes:** acceso solo a sus cursos.
 - **Profesores:** acceso a sus cursos, edición y calificación.
 - **Administradores:** acceso completo al sistema.

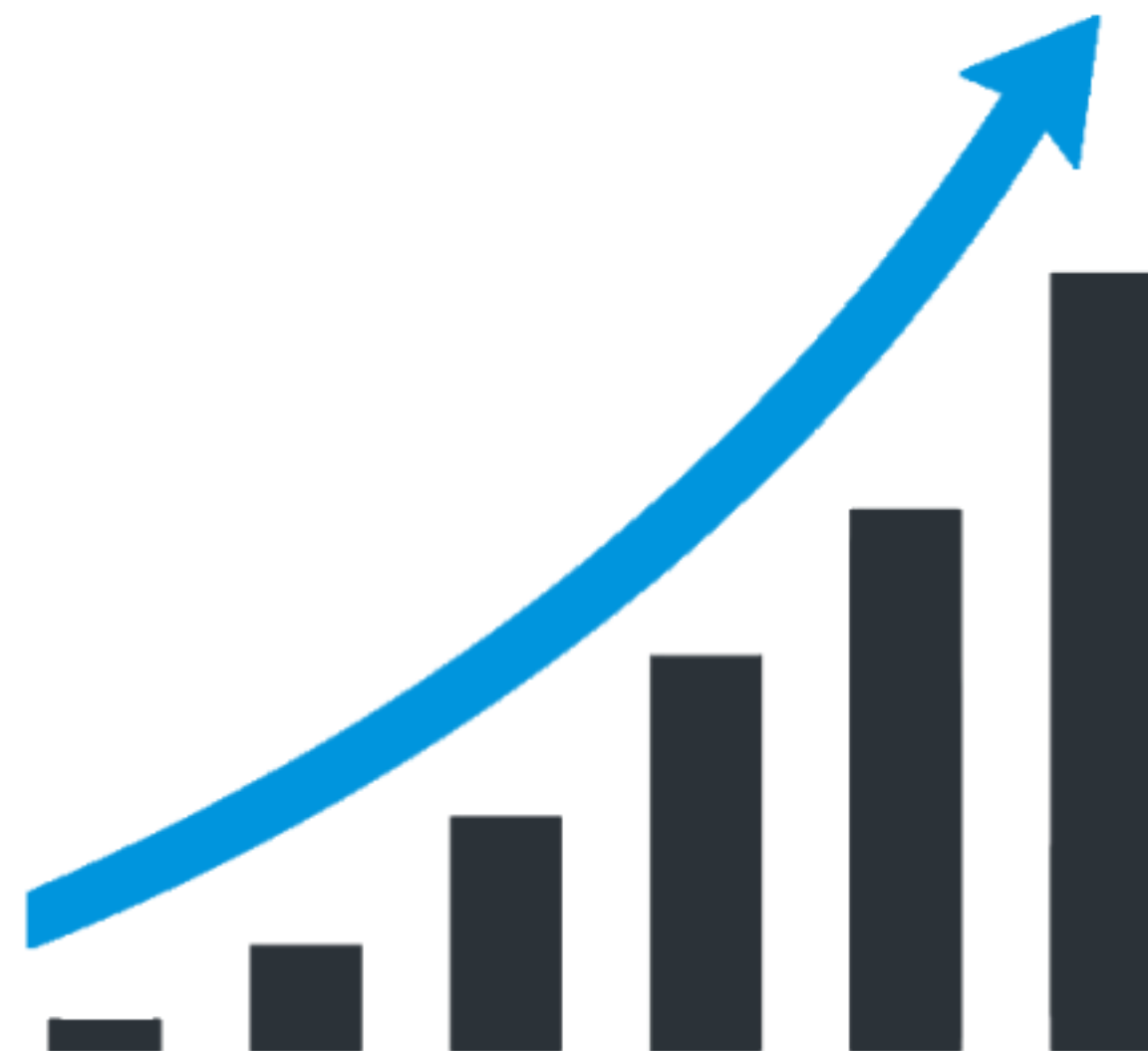
Justificación de la Solución

- **MFA** asegura una identidad robusta.
- **JWT** mejora el rendimiento y escalabilidad de sesiones.
- **RBAC** simplifica la gestión de accesos y permisos ante cambios organizacionales.



Conclusión

- La **autenticación** y **autorización** son **esenciales** para proteger las aplicaciones web.
- Es crucial **diferenciar** ambos conceptos y elegir los métodos más adecuados, como **MFA, JWT y RBAC/ABAC**, para **fortalecer la seguridad**.
- Implementar estas prácticas asegura aplicaciones web **más seguras, escalables y confiables**





Energiza!