Especialización en Back End II

# Trabajo integrador

## Contexto de negocio 

Como consultores de Digital Media nos contactan para solucionar fallas recurrentes en el **sistema de películas online**.

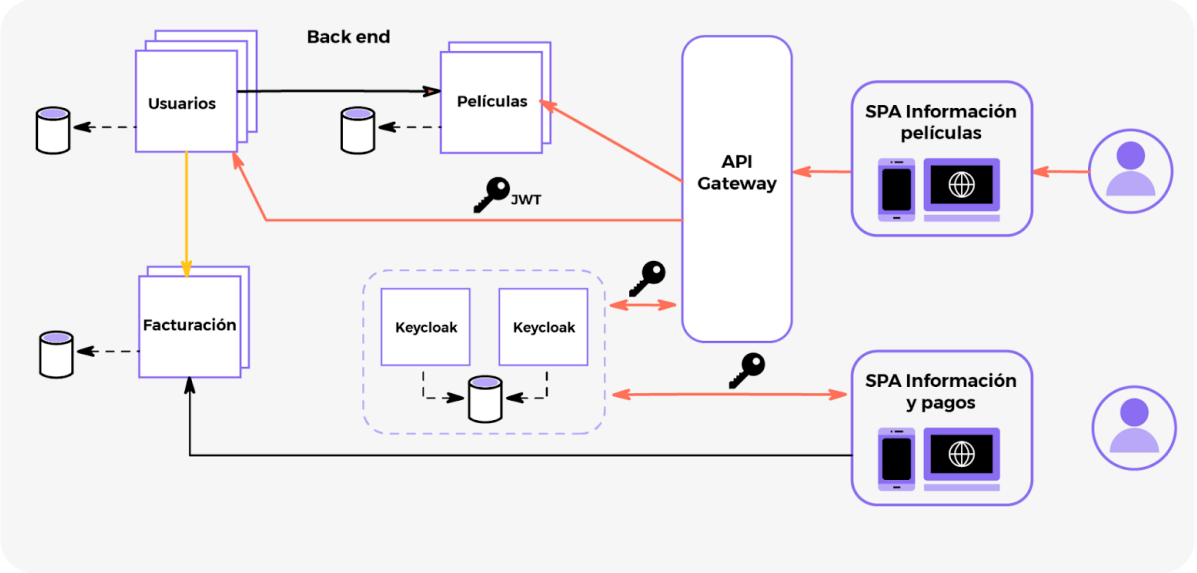
Se sabe que los usuarios y administradores no son identificados fehacientemente, es decir, las API son totalmente vulnerables, ya que se detectaron problemas en la administración de contenidos de la página, debido a la manipulación de los roles asociados al usuario común.

Adicionalmente, el mecanismo de seguridad está implementado de forma diferente en cada una de las API, por lo que el análisis y la corrección de estos tipos de vulnerabilidades es muy costoso.

Otro falla importante en este sistema está relacionado con los múltiples consumidores de esta aplicación, ya que puede ser accedida desde una página web, una aplicación en el celular e incluso en forma de API desde aplicaciones de terceros; y en cada una de estas llamadas, la validación de seguridad es diferente.

Los arquitectos de solución de este sistema plantean resolver este problema de seguridad utilizando un middleware de IAM, que centralice la gestión y lógica de seguridad de usuarios para extraer esta responsabilidad de las API. Adicionalmente, plantean la necesidad de centralizar las llamadas a todas las API actuales y futuras API, mediante un proxy intermediario, es decir, mediante un API Gateway.

Como borrador de la solución se establece lo siguiente:




Sin embargo, como consultores, participamos en una reunión interdisciplinaria con todo el área de sistemas. Entre los actores de esta meeting nos encontramos con: analistas funcionales, líderes técnicos, equipo de infraestructura, redes y seguridad de la información. Todos en esta meeting coinciden con los aspectos fundamentales de la solución, pero el equipo de seguridad de la información establece los siguientes lineamientos obligatorios:

- Identificación única y validación del usuario centralizada.
- Gestión de roles coherentes según lógica de negocio de la aplicación.
- Gestión efectiva de una sesión de usuario.
- Administrar los usuarios logueados para deshabilitarlos ante un comportamiento incorrecto.
- Comunicación segura entre los microservicios de la solución.
- Estándar de identificación de usuarios entre todos los servicios.
- Posibilidad de identificación de usuarios mediante redes sociales.
- Reducir el uso de base de datos para obtener información trivial del usuario.
- Identificar unívocamente todas las aplicaciones que usan las APIS del sistema de películas.
- Discriminar usuarios según tipo de servicio, para evitar la pérdida de facturación al permitir visualizar películas premium a usuarios comunes.

Luego de estos lineamientos, el gerente de proyectos establece un roadmap para implementar la solución.