Proyecto: TechMarket - Suite de Pruebas Automatizadas

Objetivo: Validar el correcto funcionamiento, seguridad y robustez de la API REST de TechMarket mediante pruebas manuales, automatizadas y reportes.

¿Qué es una API REST?

Una API REST es un estilo arquitectónico basado en HTTP que permite la comunicación entre sistemas mediante recursos identificados por URLs. Utiliza métodos estándar (GET, POST, PUT, DELETE) y formatos como JSON para intercambiar datos.

En este caso, la API permite:
- Gestionar productos (`/api/v1/products`)
- Registrar y autenticar usuarios (`/api/v1/auth`)

Componentes principales de una API REST

Componente	Ejemplo en TechMarket
Recurso	`/products`, `/auth`
Método HTTP	`GET`, `POST`, `PUT`, `DELETE`
Endpoint	`GET /api/v1/products`, `POST /api/v1/auth/login`
Body (JSON)	`{ "name": "Laptop", "price": 999.99 }`
Headers	`Content-Type: application/json`, `Authorization: Bearer <token>`
Códigos HTTP	`200 OK`, `201 Created`, `404 Not Found`, `401 Unauthorized`

Buenas prácticas de diseño aplicadas

Versionado de API: `/api/v1/...`
Uso de DTOs: `ProductDTO` para entrada/salida
Validación con `@Valid`
Excepciones personalizadas: `ResourceNotFoundException`
Códigos de estado correctos (201 en POST, 204 en DELETE)
Seguridad con JWT y `PasswordEncoder`
Registro con `Location` header (mejor práctica REST)

Amenazas de seguridad y mitigaciones

Amenaza	Mitigación en esta API
Acceso no autorizado	JWT en endpoints protegidos
Credenciales débiles	`@Valid` en login/register, `PasswordEncoder`
Exposición de datos	Uso de `ProductDTO` (no se expone `password`)
Usuarios duplicados	`existsByEmail()` antes de registrar
Tokens reutilizables	`tokenVersion` en `UserAccount`
Auditoría	Se agregan logs y capturas

Mecanismo de autenticación usado: JWT (JSON Web Token)