



UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

DISEÑO Y PROGRAMACIÓN DE SOFTWARE MULTIPLATAFORMA DPS104 G01L

DESAFÍO PRÁCTICO #3

DOCENTE: ING. KARENS MEDRANO

PRESENTADO POR:

MELISSA ABIGAIL FLORES ALFARO

FA220709

GABRIEL ERNESTO TOBAR ABREGO

TA220649

ENLACE DE GITHUB : <https://github.com/MelissaFloresA/Desafio3-DPS.git>

Video de funcionamiento:

https://www.canva.com/design/DAG1UAIQ5YI/4VUs7LNzk0hyhqhjFFCJkw/watch?utm_content=DAG1UAIQ5YI&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=hd92877d2fd

FUNCIONAMIENTO DE APP

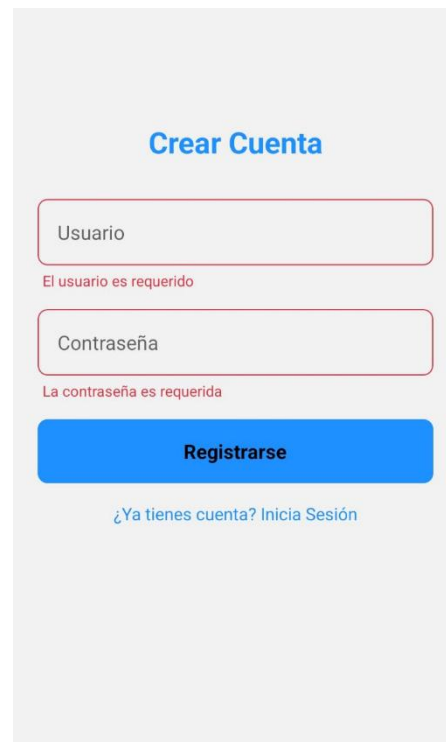


Las dos primeras pantallas incluyen validaciones que garantizan la correcta inserción de datos en la base de datos. El campo 'usuario' debe contener al menos 3 caracteres y el campo 'contraseña' un mínimo de 4 caracteres, con el fin de asegurar nombres válidos y credenciales adecuadas.



The login interface features the GM STOCK logo at the top center. Below it are two input fields: 'Usuario' and 'Contraseña'. At the bottom, there are two buttons: a blue 'Iniciar Sesión' button and a yellow 'Crear Cuenta' button.

Interfaz de Login



The registration interface has a light gray background. At the top, it says 'Crear Cuenta' in blue. Below this are two input fields: 'Usuario' and 'Contraseña'. Under the 'Usuario' field is a red error message 'El usuario es requerido'. Under the 'Contraseña' field is a red error message 'La contraseña es requerida'. At the bottom, there is a blue 'Registrarse' button and a link that says '¿Ya tienes cuenta? Inicia Sesión'.

Registro de usuario

9:22

90%



⚠ Usuario o contraseña incorrectos

chelsea

.....

Iniciar Sesión

Crear Cuenta

En caso de que el sistema muestre el mensaje 'Usuario o contraseña incorrectos', significa que las credenciales ingresadas no coinciden con el registro existente en la base de datos. Este mensaje también puede aparecer si el usuario no está registrado en el sistema. De esta manera, se evita revelar información sensible sobre la existencia o no de un usuario.

9:23

91%

GM Stock

Bienvenido Meli

Acciones Rápidas

Escanear Código QR

Ver Todos los Productos

Cerrar Sesión

¿Cómo Usar GM Stock?

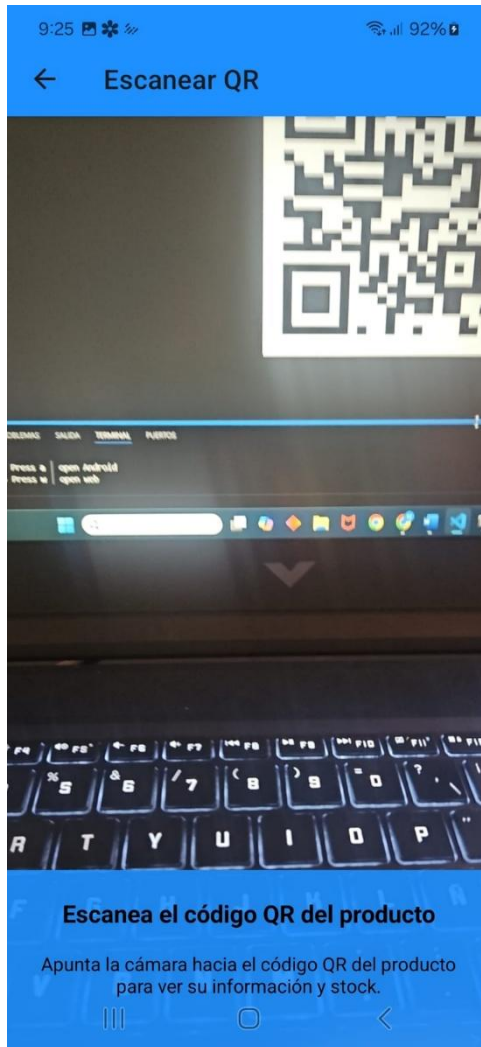
- Escanea códigos QR para ver información de productos en tienda
- Actualiza el stock desde el detalle de cada producto o escaneando
- Consulta el inventario completo en cualquier momento

Menú Principal

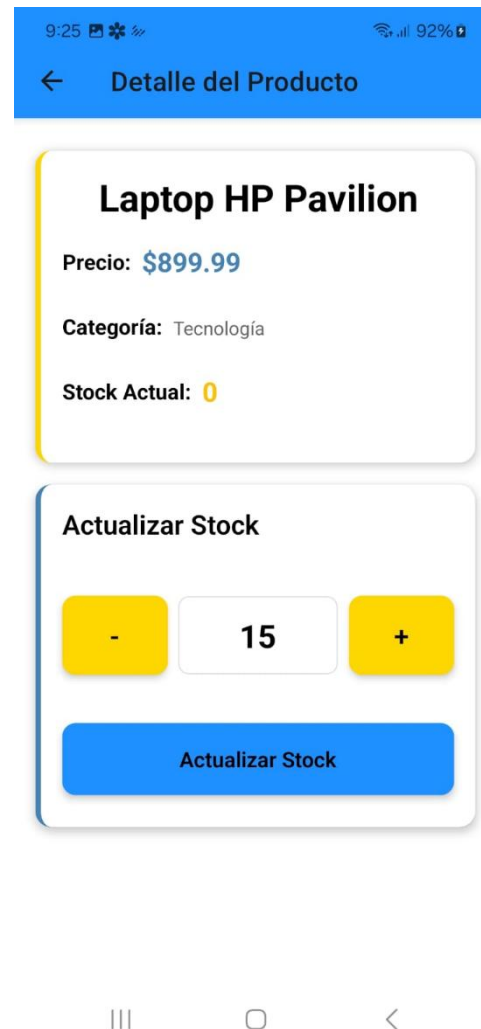
Contiene dos acciones importantes:

- Escanear Código QR: la app pedirá permisos para acceder a la cámara del dispositivo.
- Ver todos los productos: muestra la lista de productos almacenados en la base de datos

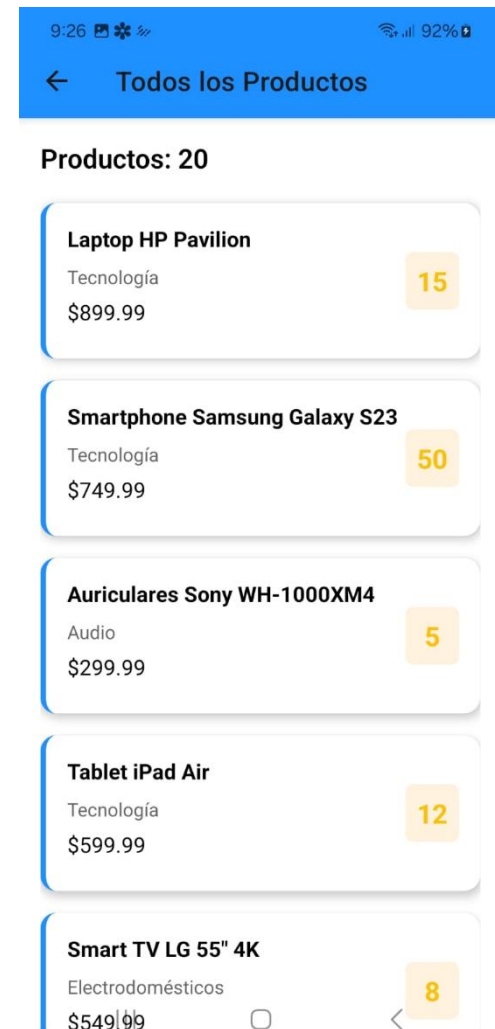
Ambas interfaces al escanear un código o darle clic a un producto de la lista se abre otra interfaz de detalle del producto, donde se puede cambiar el stock del mismo.



Interfaz de Escaneo QR

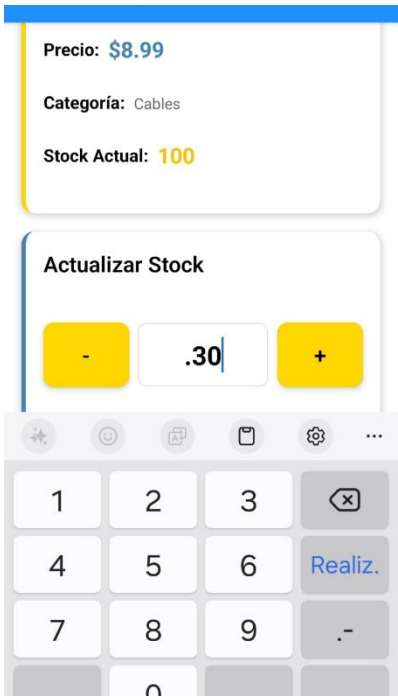


Detalles de productos y actualización de stock

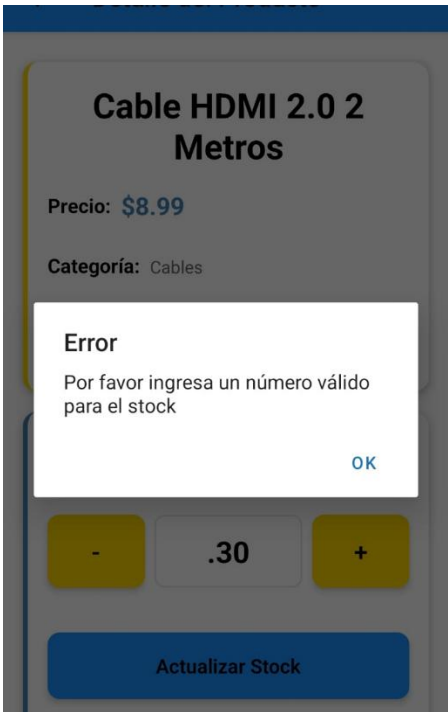


Lista de productos

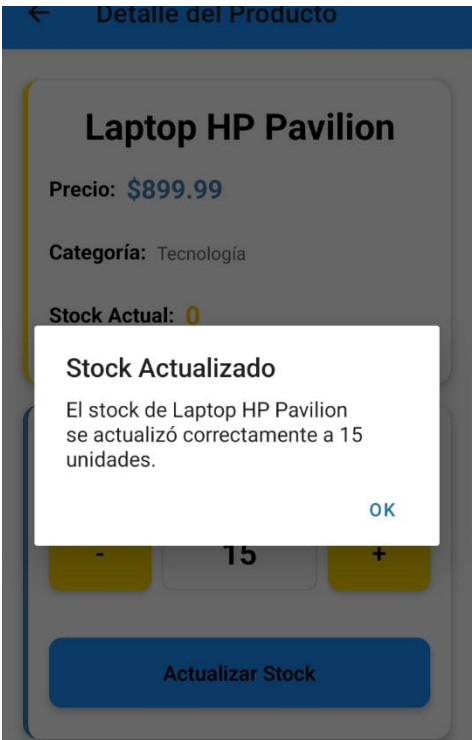
Todas las interfaces cumplen con el **100% de funcionalidad**, detallando al usuario errores en validaciones en campos de entrada y notificaciones de alerta (como actualización de stock) y cambios al instante en la base de datos.



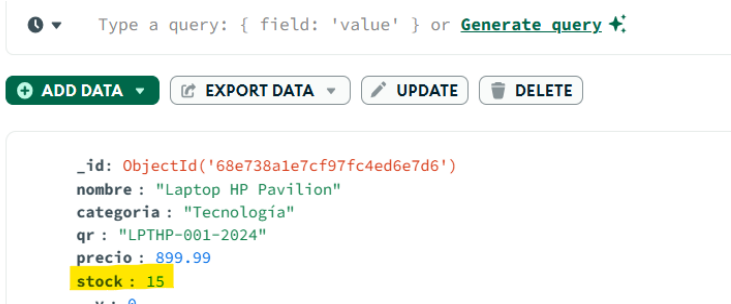
Dos formas de realizar cambio de stock: por teclado numérico o por botones



Validación ante error en cantidad de sotck



Update en base de datos al actualizar stock



API GM-Stock

El sistema cuenta con endpoints para el registro y autenticación de usuarios, asegurando el acceso mediante tokens JWT.

- **POST /api/auth/register:** Permite registrar un nuevo usuario proporcionando nombre de usuario y contraseña.
- **POST /api/auth/login:** Autentica un usuario existente y devuelve un token JWT para acceder a los recursos protegidos.

Otros endpoint para gestión de productos.

- **GET /api/products/obtener:** Devuelve el listado completo de productos registrados:
- **GET /api/products/obtener/:id :** Permite consultar la información detallada de un producto específico.
- **POST /api/products/actualizar/:id:** Actualizar stock de producto.

Cada solicitud válida devuelve los datos del usuario autenticado junto con su token. Cada vez que el usuario realiza una solicitud a un endpoint protegido, debe incluir el token en los encabezados, el servidor valida la firma del token y, si es válido, permite el acceso a los recursos; de lo contrario, lo rechaza. Esto evita que usuarios no autenticados o sin permisos accedan a la información.

La inserción de productos se hace automáticamente, la app podrá actualizar stock de los productos creados.

El backend implementa buenas prácticas de seguridad, entre ellas:

- **JWT:** Tokens firmados con una clave secreta.
- **bcrypt:** Hash seguro de contraseñas.
- **Validaciones:** Control de campos requeridos y tipos de datos.
- **Manejo seguro de errores:** Los mensajes no exponen información sensible.