**ETAPA 4: SEGURIDAD E INTEGRIDAD**

En esta etapa se verificaron las medidas de seguridad y las restricciones de integridad de la base de datos *Pedido\_Envio*. Se realizaron pruebas para validar las restricciones definidas (PK, FK, CHECK y UNIQUE), así como la creación de un usuario con privilegios mínimos y el uso de vistas para ocultar información sensible.

1. **Creación del usuario y permisos mínimos**

Se creó el usuario *usuario\_prueba* con permisos mínimos para acceder a la base de datos *Pedido\_Envio.*

A screenshot of a computer code

AI-generated content may be incorrect.

Este usuario puede consultar, insertar y modificar registros, pero no puede modificar la estructura de la base.

A screenshot of a computer

AI-generated content may be incorrect.

Se comprueba el acceso restringido de este nuevo usuario mediante las siguientes pruebas:

* PRUEBA 1 — Intento de DELETE denegado



Resultado obtenido:

*Error Code: 1142. DELETE command denied to user 'usuario\_prueba'@'localhost' for table 'pedido'*

El usuario no tiene privilegio de eliminación directa de registros, cumpliendo el principio de mínimo privilegio.

* PRUEBA 2 — Intento de DROP TABLE denegado



Resultado obtenido:

*Error Code: 1142. DROP command denied to user 'usuario\_prueba'@'localhost' for table 'envio'*

El usuario no puede borrar estructuras de base de datos. Solo el administrador (root) puede realizar esta acción.

* PRUEBA 3 — Intento de ALTER TABLE denegado



Resultado obtenido:

*Error Code: 1142. ALTER command denied to user 'usuario\_prueba'@'localhost' for table 'pedido'*

La base de datos bloquea los intentos de modificación de estructura, garantizando la estabilidad del modelo y la integridad del sistema.

1. **Vistas para ocultar información sensible**

Se crearon dos vistas para restringir el acceso a información sensible y mostrar solo registros activos:

A screenshot of a computer code

AI-generated content may be incorrect.

Mediante esta vista se pueden consultar los pedidos sin mostrar los campos total y eliminado.  
El campo total contiene valores económicos que pueden considerarse información confidencial o no relevante según el rol del usuario, por lo que su exclusión reduce riesgos de exposición o análisis indebido.  
El campo eliminado refleja un estado interno del sistema, no destinado al usuario final. Ocultarlo evita mostrar registros inactivos o dar acceso a información administrativa.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer code

AI-generated content may be incorrect.

Esta vista muestra los envíos activos, ocultando los campos costo y eliminado.  
El primero contiene información económica interna y el segundo indica registros inactivos no visibles para el usuario final.  
Ocultar ambos campos permite simplificar el acceso y proteger información administrativa o sensible del sistema.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Pruebas de integridad**

**PRUEBA 1 — Violación de PRIMARY KEY**

La PK garantiza que no se repitan valores en la columna id de la tabla Pedido.

Para verificar su correcto funcionamiento, se inserta un pedido válido y luego se intenta duplicar el mismo valor de clave primaria.  
El sistema arroja un error de duplicidad, demostrando que la restricción funciona correctamente.

A close up of some words

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A close up of a white background

AI-generated content may be incorrect.

Resultado obtenido:

*Error Code: 1062. Duplicate entry '1' for key 'pedido.PRIMARY'*

**PRUEBA 2 — Violación de FOREIGN KEY**

Los campos total y costo no pueden ser negativos. La restricción CHECK evita valores inválidos en montos numéricos. Se verifica el funcionamiento de estas restricciones en las tablas Envio y Pedido insertando registros con dichos campos con valores negativos para comprobar el buen funcionamiento. Se sistema devuelve errores de violación de Check.

A close-up of a computer screen

AI-generated content may be incorrect.

Resultado obtenido:

*Error Code: 1452. Cannot add or update a child row: a foreign key constraint fails (`pedido\_envio`.`pedido`, CONSTRAINT `pedido\_ibfk\_1` FOREIGN KEY (`envio`) REFERENCES `envio` (`id`))*

**PRUEBA 3 — Violación de UNIQUE**

El campo tracking de la tabla Envio debe ser único para cada registro.  
La restricción UNIQUE impide que se repita el código de seguimiento de un envío.  
Para comprobar su funcionamiento, se inserta un registro válido y luego se intenta duplicar el mismo valor de tracking.  
El sistema devuelve un error de duplicidad, confirmando el correcto funcionamiento de la restricción.

A close-up of a computer code

AI-generated content may be incorrect.

A close up of a price

AI-generated content may be incorrect.

A close up of text

AI-generated content may be incorrect.

Resultado obtenido:

*Error Code: 1062. Duplicate entry 'T001' for key 'envio.tracking'*

**PRUEBA 4 — Violación de CHECK (valor negativo)**

Los campos total en Pedido y costo en Envio no pueden contener valores negativos.  
La restricción CHECK evita la inserción de montos no válidos en dichas columnas.  
Se verifica su funcionamiento intentando registrar valores negativos en ambos campos, ante lo cual el sistema devuelve un error de violación de la restricción, demostrando su efectividad.

A computer code with numbers and letters

AI-generated content may be incorrect.

Resultados obtenidos:

*Error Code: 3819. Check constraint 'envio\_chk\_1' is violated.*

*Error Code: 3819. Check constraint 'pedido\_chk\_1' is violated.*

1. **Consulta Segura en JAVA (PreparedStatement)**

Se implementó una consulta parametrizada usando PreparedStatement y una llamada a un procedimiento almacenado (sp\_get\_pedido\_por\_numero) sin SQL dinámico. Ambos mecanismos tratan los parámetros como datos (no como código), previniendo SQL Injection.

**Código Java**

**A computer screen shot of text

AI-generated content may be incorrect.**

**A computer screen shot of a program code

AI-generated content may be incorrect.**

**A screen shot of a computer program

AI-generated content may be incorrect.**

**Pruebas realizadas:**

* Input válido: PED-TEST-001 → devuelve el pedido.
* Intento clásico: '' OR '1'='1 → no devuelve registros (el payload se busca literalmente).
* Intento destructivo: PED-TEST-001'; DROP TABLE Pedido; -- → no borra la tabla; no se ejecuta el DROP.
* Llamada SP con payload: sp\_get\_pedido\_por\_numero("' OR '1'='1") → no devuelve registros.

A computer screen shot of a black screen

AI-generated content may be incorrect.

**Conclusión:** La parametrización con PreparedStatement y el uso de procedimientos sin SQL dinámico impiden que datos de entrada se interpreten como instrucciones SQL maliciosas.