

SENA

05/09/2024

MÓDULOS CODIFICADOS Y PROBADOS

Instructor: Tatiana Forero

Aprendices: Juan Gonzalez

Evidencia: GA7-220501096-AA3-EV02.

Centro: Industria y construcción regional del Tolima

Ficha: 2721462



```
else if (i==2)
{
    var atpos=inputs[i].indexOf("@");
    var dotpos=inputs[i].lastIndexOf(".");
    if (atpos<1 || dotpos<atpos+2 || dotpos>inputs[i].lastIndexOf(".", 1))
    document.getElementById('errEmail').innerHTML = "El correo no es válido";
    else
    document.getElementById(div).innerHTML = "El correo no es válido";
}
```

Tabla de Contenido

1. Introducción

1.1. Propósito

1.2. Referencias

2. Módulos codificados y probados

2.1. Caso de uso 1

2.1.1. Descripción de Caso de Uso

2.1.2. Diagrama de Caso de Uso

2.1.3. Plantillas de Caso de Uso

2.1.4. Pruebas en Postman

3. Conclusión

1. Introducción:

El módulo de "Gestión de Usuarios y Permisos" es fundamental en cualquier sistema que maneje información sensible y requiere diferentes niveles de acceso. Este módulo permite administrar de manera efectiva a los usuarios del sistema, asegurando que solo personas autorizadas puedan acceder a determinadas funcionalidades y datos. En el contexto de una aplicación de gestión de vehículos, donde la información financiera y de inventario es crítica, establecer un control adecuado sobre los usuarios y sus permisos es esencial para garantizar la seguridad y el buen funcionamiento del sistema.

1.1. Propósito:

El propósito de este documento es presentar y detallar el funcionamiento del módulo de "Gestión de Usuarios y Permisos" mediante un diagrama de caso de uso. Se busca describir cómo los diferentes actores (administradores, vendedores, y otros usuarios) interactúan con las funcionalidades clave de este módulo. El documento también tiene como objetivo proporcionar una visión clara de las relaciones y restricciones entre las distintas acciones, asegurando que los usuarios tengan el acceso adecuado según su rol dentro del sistema.

1.2. Referencias

2. Módulos codificados y probados

2.1. Caso de uso

2.1.1. Descripción de Requisito Administrador de empleados:

RF1. Administración de Usuarios:

- El sistema debe permitir la creación, modificación, y eliminación de usuarios.
- El sistema debe permitir la asignación de roles a cada usuario (ej. Administrador, Vendedor, Usuario estándar).

RF2. Asignación de Permisos:

- El sistema debe permitir definir y asignar permisos específicos a los usuarios basados en su rol.
- Los permisos deben controlar el acceso a funciones críticas del sistema, como la visualización de datos sensibles, la modificación de inventario, y la gestión de transacciones.

RF3. Control de Acceso:

- El sistema debe garantizar que solo los usuarios autorizados puedan acceder a las funciones y datos correspondientes a su nivel de permisos.
- Los administradores deben tener acceso completo al sistema, mientras que los vendedores y otros usuarios deben tener acceso limitado a funciones específicas según sus roles.

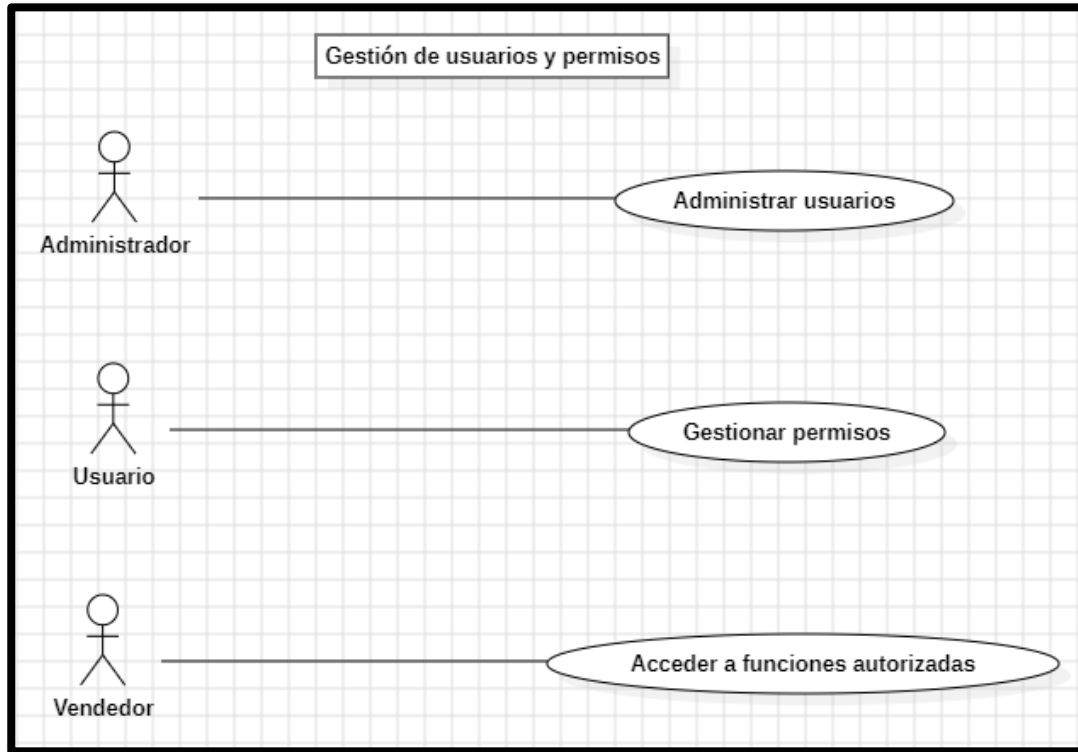
RF4. Auditoría de Acceso:

- El sistema debe registrar todas las acciones importantes realizadas por los usuarios, como modificaciones de datos, cambios de permisos y acceso a información sensible.
- Debe ser posible generar informes de auditoría para revisar las acciones realizadas por cada usuario.

RF5. Gestión de Roles:

- El sistema debe permitir la creación de nuevos roles personalizados con permisos específicos.
- Los roles predeterminados deben incluir Administrador, Vendedor, y Usuario estándar, con la posibilidad de ser modificados según las necesidades del negocio.

2.1.2. Diagrama Caso de Uso



2.1.3. Plantillas de Caso de Uso

- Plantilla Caso de Uso: Administrar Usuarios

| Nombre del Caso de Uso | Administrar Usuarios |
|------------------------|--|
| ID | CU-001 |
| Descripción | El administrador gestiona los usuarios del sistema, pudiendo crear nuevos usuarios, modificar la información de los existentes o eliminarlos. |
| Actores Principales | Administrador |
| Precondiciones | El administrador debe haber iniciado sesión en el sistema. |
| Postcondiciones | El usuario se ha creado, modificado o eliminado correctamente. |
| Flujo Principal | <ol style="list-style-type: none">1. El administrador accede al módulo de gestión de usuarios.2. El administrador selecciona la opción de crear, modificar o eliminar un usuario.3. El sistema muestra un formulario para ingresar/modificar la información del usuario (nombre, correo, contraseña, rol, etc.).4. El administrador completa o edita la información y confirma la acción.5. El sistema guarda los cambios y muestra un mensaje de éxito. |
| Excepciones | <ul style="list-style-type: none">- Problema de conexión a la base de datos.- El sistema muestra un mensaje de error indicando la falta de conexión y sugiere intentar más tarde. |

- Plantilla de Caso de Uso: Consultar usuarios

| Nombre del Caso de Uso | Consultar usuarios |
|------------------------|---|
| ID | CU-002 |
| Descripción | Permite a los administradores consultar la información de los usuarios en el sistema. |
| Actores Principales | administrador |
| Actores Secundarios | Base de Datos del Sistema |
| Precondiciones | El administrador ha iniciado sesión en el sistema. |
| Postcondiciones | La información del usuario consultado es visualizada por el administrador. |
| Flujo Principal | <ol style="list-style-type: none">1. El administrador accede a la función de gestión de usuario.2. Selecciona la opción para consultar la información de los usuarios. |

| | |
|-------------------------------|---|
| Nombre del Caso de Uso | Consultar usuarios |
| | 3. Introduce criterios de búsqueda (nombre, ID, departamento, etc.). 4. El sistema muestra la información del usuario solicitado. |
| Flujo Alternativo | - Si no se encuentra al usuario solicitado, el sistema muestra un mensaje indicando que no se encontraron resultados. |
| Excepciones | - Problema de conexión a la base de datos. - El sistema muestra un mensaje de error indicando la falta de conexión y sugiere intentar más tarde. |
| Reglas de Negocio | Solo los administradores pueden consultar información detallada de los usuarios. |
| Requisitos Especiales | Funcionalidades de búsqueda avanzada y filtros. |

- **Plantilla de Caso de Uso: Agregar usuarios**

| | |
|-------------------------------|--|
| Nombre del Caso de Uso | Agregar usuarios |
| ID | CU-003 |
| Descripción | Permite a los gerentes agregar nuevos empleados al sistema. |
| Actores Principales | Administrador |
| Precondiciones | El administrador ha iniciado sesión en el sistema. |
| Postcondiciones | La información del nuevo usuario está registrada en el sistema. |
| Flujo Principal | 1. El administrador accede a la función de gestión de usuarios. 2. Selecciona la opción para agregar un nuevo usuario. 3. Introduce la información requerida del usuario (nombre, dirección, posición, etc.). 4. Guarda la información del nuevo usuario. 5. El sistema confirma la creación del nuevo usuario y actualiza la base de datos. |
| Flujo Alternativo | Si la información introducida está incompleta o es incorrecta, el sistema muestra un mensaje de error y solicita correcciones. |
| Excepciones | - Problema de conexión a la base de datos - El sistema muestra un mensaje de error indicando la falta de conexión y sugiere intentar más tarde. |
| Reglas de Negocio | Solo los gerentes pueden agregar usuarios. |
| Requisitos Especiales | Validaciones para los datos introducidos (por ejemplo, formato del correo electrónico, longitud del teléfono, etc.). |

- **Plantilla de Caso de Uso: Eliminar usuarios**

| | |
|-------------------------------|--|
| Nombre del Caso de Uso | Eliminar usuarios |
| ID | CU-004 |
| Descripción | Permite al administrador eliminar usuarios del sistema. |
| Actores Principales | Administrador |
| Precondiciones | El administrador ha iniciado sesión en el sistema. |
| Postcondiciones | La información del usuario está eliminada del sistema. |
| Flujo Principal | <ol style="list-style-type: none"> 1. El gerente accede a la función de gestión de usuario. 2. Selecciona la opción para eliminar un usuario. 3. Introduce la identificación del usuario a eliminar. 4. Confirma la eliminación del usuario. 5. El sistema elimina la información del usuario y actualiza la base de datos. |
| Flujo Alternativo | Si la identificación del usuario es incorrecta o no existe, el sistema muestra un mensaje de error y solicita correcciones. |
| Excepciones | <ul style="list-style-type: none"> - Problema de conexión a la base de datos. - El sistema muestra un mensaje de error indicando la falta de conexión y sugiere intentar más tarde. |
| Reglas de Negocio | Solo el administrador pueden eliminar usuarios. |
| Requisitos Especiales | Confirmación antes de la eliminación para evitar errores. |

- **Plantilla de Caso de Uso: Modificar usuarios**

| | |
|-------------------------------|---|
| Nombre del Caso de Uso | Modificar usuario |
| ID | CU-005 |
| Descripción | Permite a los administradores modificar la información de los usuarios en el sistema. |
| Actores Principales | Administrador |
| Precondiciones | El administrador ha iniciado sesión en el sistema. |
| Postcondiciones | La información del usuario está actualizada en el sistema. |
| Flujo Principal | <ol style="list-style-type: none"> 1. El administrador accede a la función de gestión de usuarios. 2. Selecciona la opción para modificar un usuario. 3. Introduce la identificación del usuario a modificar. 4. El sistema muestra la información actual del usuario. 5. El administrador modifica la información del usuarios(nombre, dirección,posición, etc.). 6. Guarda la información modificada. 7. El sistema confirma la modificación y actualiza la base de datos. |
| Flujo Alternativo | - Si la identificación del usuario es incorrecta o no existe, el sistema muestra un mensaje de error y solicita correcciones. |

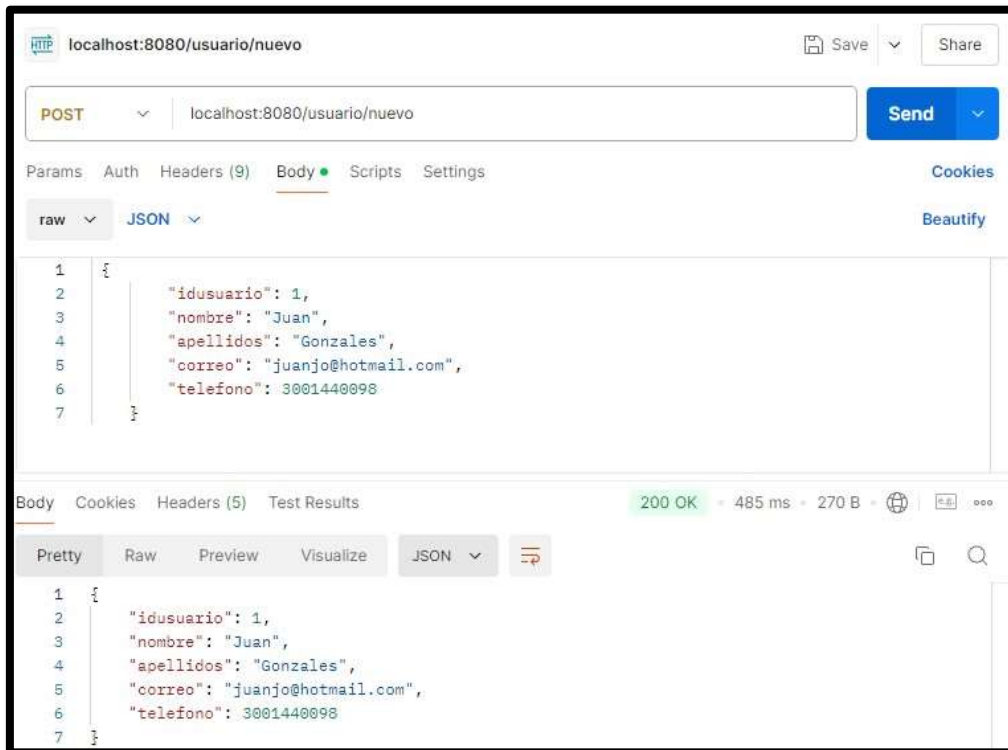
| Nombre del Caso de Uso | Modificar usuarios |
|------------------------|---|
| Excepciones | <ul style="list-style-type: none"> - Problema de conexión a la base de datos. - El sistema muestra un mensaje de error indicando la falta de conexión y sugiere intentar más tarde. |
| Reglas de Negocio | Solo los administradores pueden modificar la información de los usuarios. |
| Requisitos Especiales | Validaciones para los datos modificados (por ejemplo, formato del correo electrónico, longitud del teléfono, etc.). |
| Puntos de Extensión | Notificaciones a los usuarios sobre los cambios en su información. |

- Plantilla de Caso de Uso: Asignación de Permisos

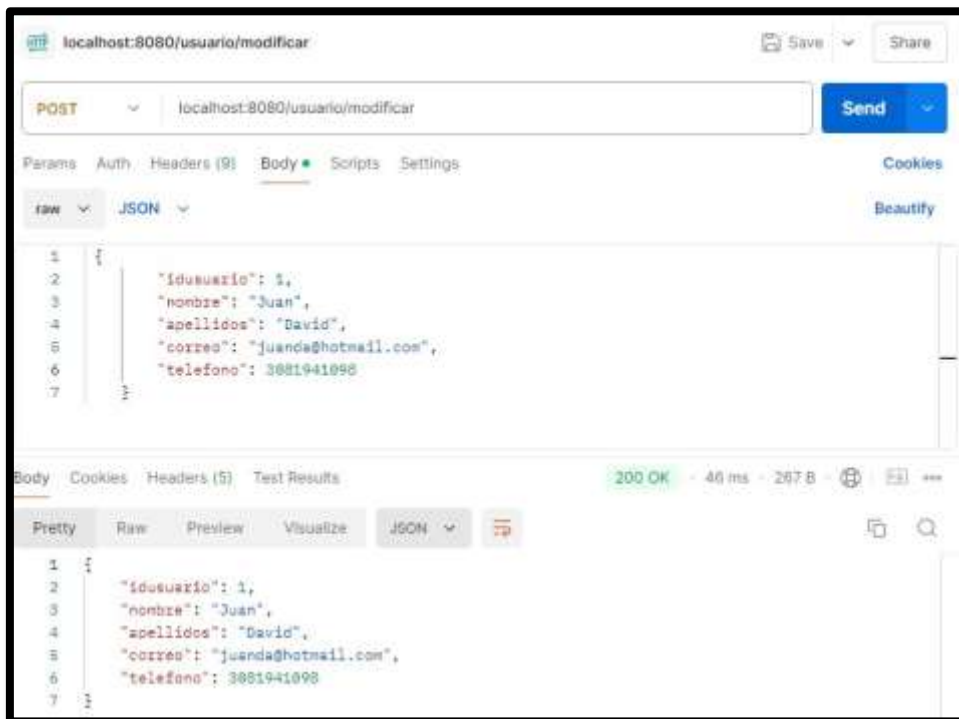
| Nombre del Caso de Uso | Asignación de Permisos |
|------------------------|---|
| ID | CU-006 |
| Descripción | El administrador asigna o modifica los permisos de acceso para los usuarios en función de sus roles. |
| Actores Principales | Administrador |
| Precondiciones | El administrador debe haber iniciado sesión y debe existir al menos un usuario en el sistema. |
| Postcondiciones | Los permisos del usuario se han actualizado correctamente. |
| Flujo Principal | <ol style="list-style-type: none"> 1. El administrador accede al perfil de un usuario. 2. El administrador selecciona la opción de editar permisos. 3. El sistema muestra las opciones de permisos disponibles para el rol del usuario. 4. El administrador selecciona o modifica los permisos deseados. 5. El administrador guarda los cambios. 6. El sistema actualiza los permisos del usuario y confirma la acción. |

2.1.4. Pruebas en Postman

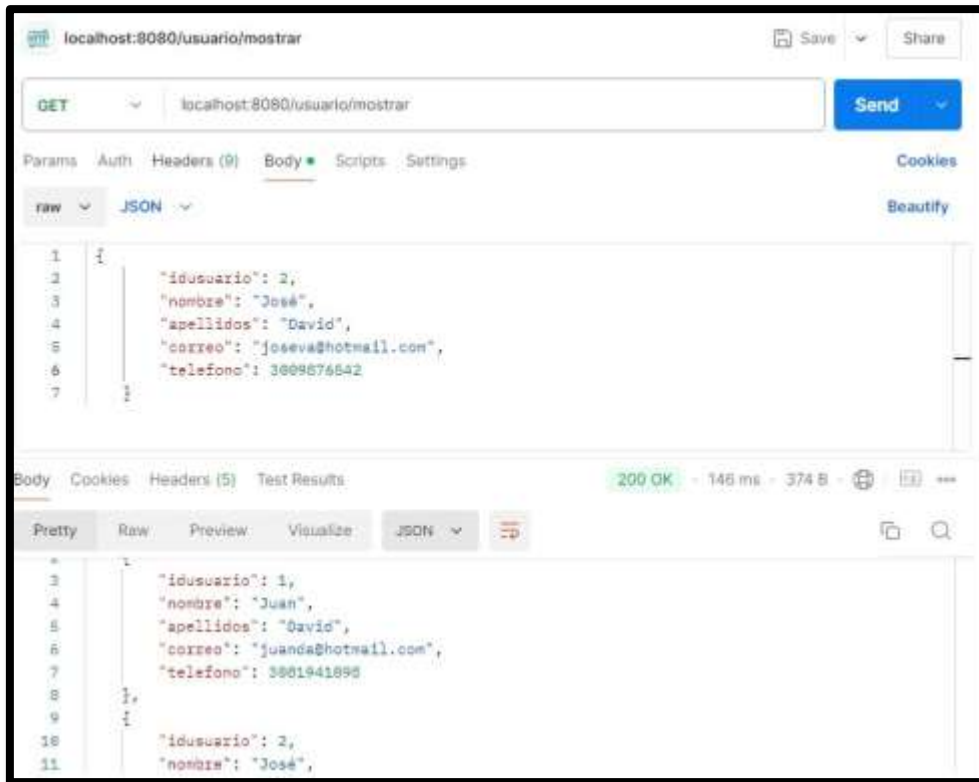
- Agregar usuarios



- Modificar usuario



- Mostrar usuario



localhost:8080/usuario/mostrar

GET localhost:8080/usuario/mostrar

Params Auth Headers (9) Body Scripts Settings

raw JSON Beautify

```
1 {
2   "idusuario": 2,
3   "nombre": "José",
4   "apellidos": "David",
5   "correo": "joseva@hotmail.com",
6   "telefono": 3609876542
7 }
```

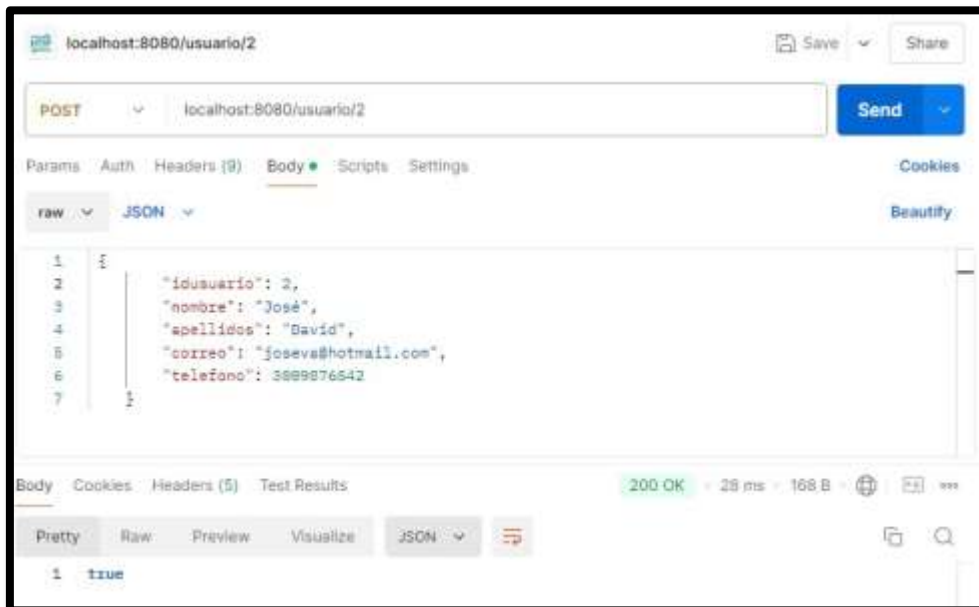
Body Cookies Headers (5) Test Results

200 OK - 146 ms - 374 B

Pretty Raw Preview Visualize JSON

```
1 {
2   "idusuario": 1,
3   "nombre": "Juan",
4   "apellidos": "David",
5   "correo": "juanda@hotmail.com",
6   "telefono": 3601941896
7 },
8 {
9   "idusuario": 2,
10  "nombre": "José",
11  "apellidos": "David",
12  "correo": "joseva@hotmail.com",
13  "telefono": 3609876542
14 }
```

- Eliminar usuario



localhost:8080/usuario/2

POST localhost:8080/usuario/2

Params Auth Headers (9) Body Scripts Settings

raw JSON Beautify

```
1 {
2   "idusuario": 2,
3   "nombre": "José",
4   "apellidos": "David",
5   "correo": "joseva@hotmail.com",
6   "telefono": 3609876542
7 }
```

Body Cookies Headers (5) Test Results

200 OK - 26 ms - 168 B

Pretty Raw Preview Visualize JSON

```
1 true
```

- Valor Único en correo electrónico

localhost:8080/usuario/nuevo

POST localhost:8080/usuario/nuevo

Send

Params Auth Headers (9) Body Scripts Settings

raw JSON Beautify

```
1 {
2   "idusuario": 2,
3   "nombre": "José",
4   "apellidos": "David",
5   "correo": "joseva@hotmail.com",
6   "telefono": 3009870999
7 }
```

Body Cookies Headers (4) Test Results

500 Internal Server Error 127 ms 12.1 KB

Pretty Raw Preview Visualize JSON

```
1 {
2   "timestamp": "2024-09-08T13:33:04.228+00:00",
3   "status": 500,
4   "error": "Internal Server Error",
5   "trace": "org.springframework.dao.DataIntegrityViolationException: could not execute statement [Duplicate entry 'joseva@hotmail.com' for key UK_ded6c93tikjuarino@vvywlb0`] [insert into empleado (apellidos,correo,nombres,
```

- Datos no nulos en nombre

localhost:8080/usuario/nuevo

POST localhost:8080/usuario/nuevo

Send

Params Auth Headers (9) Body Scripts Settings

raw JSON Beautify

```
1 {
2   "idusuario": 4,
3   "apellidos": "Ferradanez",
4   "correo": "ferradan@hotmail.com",
5   "telefono": 3009998888
6 }
```

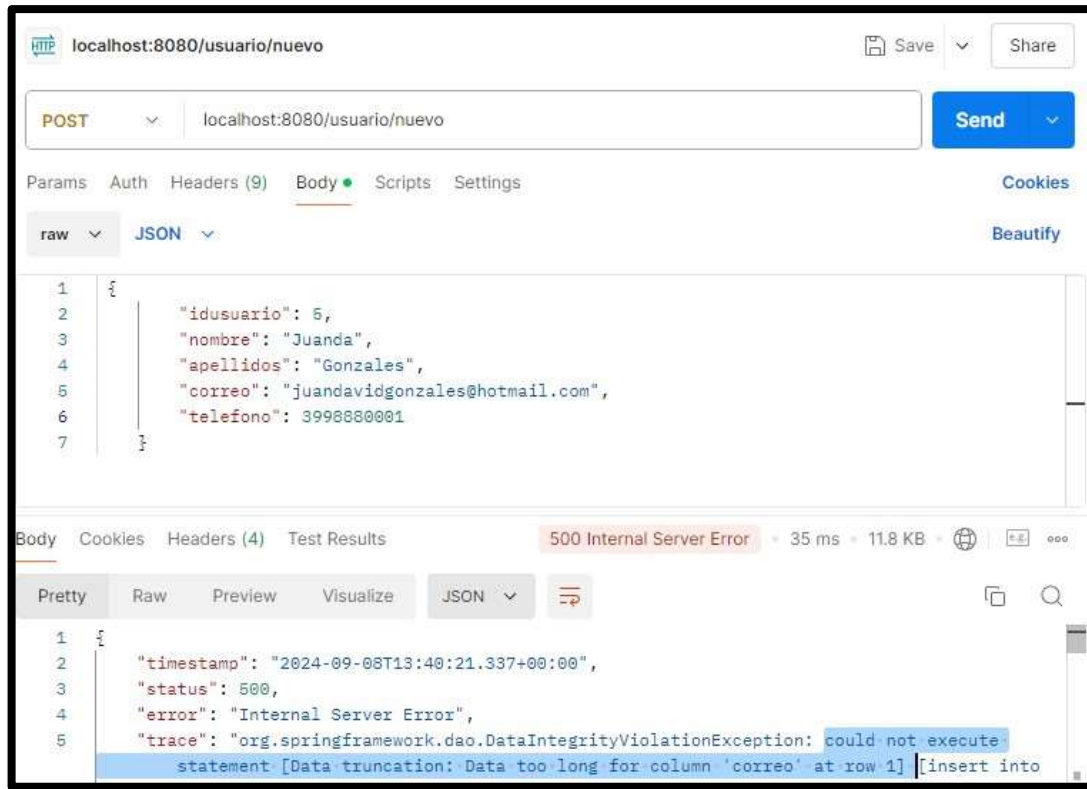
Body Cookies Headers (4) Test Results

500 Internal Server Error 22 ms 12.54 KB

Pretty Raw Preview Visualize JSON

```
1 {
2   "timestamp": "2024-09-08T13:35:59.761+00:00",
3   "status": 500,
4   "error": "Internal Server Error",
5   "trace": "org.springframework.dao.DataIntegrityViolationException: not-null property references a null or transient value: com. .... nombre\r\n\tat org.springframework.orm.jpa.vendor.HibernateJpaDialect.
```

- Mayor longitud en correo



3. Conclusión:

El módulo de "Gestión de Usuarios y Permisos" es vital para mantener la integridad y seguridad de la aplicación de gestión de vehículos. A través del diagrama de caso de uso, se ha mostrado cómo diferentes actores interactúan con este módulo, garantizando un control adecuado sobre quién puede realizar ciertas acciones. Al implementar correctamente este módulo, se asegura que la aplicación no solo sea eficiente en sus operaciones, sino también segura y confiable para todos los usuarios involucrados. Este documento sienta las bases para futuras mejoras y garantiza que el sistema cumpla con los estándares de seguridad requeridos.