**Entrega N° 1**

Consigna:

Implementar en el proyecto ecommerce facilitado al inicio del curso un CRUD de usuarios, junto con un sistema de Autenticación y Autorización.

Aspectos a Incluir:

1. **Modelo de Usuario:**
   * Crear un modelo

User

 que contenga los siguientes campos:

* + - first\_name

: String

* + - last\_name

: String

* + - email

: String (debe ser único)

* + - age

: Number

* + - password

: String (en formato hash)

* + - cart

: Id con referencia a

Carts

* + - role

: String (valor por defecto: 'user')

1. **Encriptación de Contraseña:**
   * Utilizar el paquete

bcrypt

 para encriptar la contraseña del usuario mediante el método

hashSync

.

1. **Estrategias de Passport:**
   * Desarrollar las estrategias de Passport para que funcionen con el modelo de usuarios creado.
2. **Sistema de Login:**
   * Implementar un sistema de login del usuario que trabaje con JWT (JSON Web Tokens).
3. **Ruta de Validación:**
   * Agregar al router

/api/sessions/

 la ruta

/current

, que validará al usuario logueado y devolverá en una respuesta sus datos asociados al JWT.

Formato de Entrega:

* Link al repositorio de GitHub con el proyecto completo, sin incluir la carpeta

node\_modules

.

Esta actividad es una parte fundamental de la preparación para la entrega del proyecto final y se centra en la implementación de mecanismos de seguridad y gestión de usuarios, que son esenciales para el desarrollo de aplicaciones backend robustas y seguras.

**Criterios:**

* **Modelo de Usuario y Encriptación de Contraseña:**

Crear modelo User con los campos especificados y se ha implementado la encriptación de la contraseña utilizando bcrypt.hashSync.

Que el modelo User incluya todos los campos requeridos.

Que la contraseña se encripte correctamente y se almacene en la base de datos de forma segura.

* **Estrategias de Passport para Autorización y Autenticación:**

Que se desarrollen y configuren las estrategias de Passport para el modelo de usuarios definido.

Que las estrategias de Passport están correctamente configuradas para la autenticación y autorización de usuarios.

Que se haya implementado una estrategia para la autenticación del usuario mediante JWT.

* **Sistema de Login y Generación de Token JWT:**

Que el sistema de login permita a los usuarios autenticarse y generar un token JWT válido.

Que los usuarios pueden iniciar sesión de manera exitosa y se les asigna un token JWT.

Que el token JWT sea válido y pueda utilizarse para realizar acciones protegidas en la aplicación.

* **Estrategia "Current" y Endpoint /api/sessions/current:**

Que se implemente una estrategia "current" que valide al usuario logueado y extraiga sus datos mediante el endpoint /api/sessions/current.

Que la estrategia "current" permita extraer el usuario asociado al token JWT de manera efectiva.

Que en caso de token inválido o inexistente, se devuelva un error apropiado de Passport.

Que el endpoint /api/sessions/current funcione correctamente y devuelva los datos del usuario asociado al token JWT.

Que la validación del usuario en el endpoint sea precisa y segura.

[Criterios de evaluación](https://drive.google.com/file/d/1oYDzesWHjivQB4KfWMVrxIdOM5bVbD7C/view?usp=drive_link)