**DESARROLLO SESION I Y II INGENIERIA WEB**

**Alumno**

Daniel Sebastián Ramos Moreno

**Profesora**

Olga Lucia Roa Bohórquez

**Clase**

Ingeniera Web

Universidad Manuela Beltrán

2025

**DESARROLLO SESION I**

**1.Investiga sobre los diferentes diseños que se deben realizar en un proyecto web. Desarrollando el proceso propuesto en la guía de laboratorio en grupos de trabajo buscando trabajar competencias como el trabajo en equipo y la comunicación entre pares académicos**

### **1. Diseño de Arquitectura de Información (IA)**

* Organiza la estructura del contenido del sitio.
* Define el mapa del sitio y los flujos de navegación.
* Se crean esquemas de jerarquía y relaciones entre páginas.

**Proceso:**

* Lluvia de ideas en equipo sobre la organización de la información.
* Creación de esquemas y diagramas de flujo.
* Validación con pruebas de usuarios o feedback entre pares.

### ****2. Diseño UX (Experiencia de Usuario)****

* Define la interacción del usuario con la web.
* Asegura accesibilidad, usabilidad y satisfacción del usuario.
* Incluye la creación de wireframes y prototipos.

**Proceso:**

* Investigación sobre el usuario objetivo.
* Creación de bocetos y wireframes (pueden ser en papel o herramientas como Figma).
* Evaluación mediante pruebas de usabilidad.

### ****3. Diseño UI (Interfaz de Usuario)****

* Define la apariencia visual del sitio (colores, tipografía, iconografía).
* Se basa en principios de diseño gráfico y branding.

**Proceso:**

* Creación de moodboards e identificación de la identidad visual.
* Diseño de interfaces con herramientas como Adobe XD o Figma.
* Revisión y ajuste con base en feedback del equipo.

### ****4. Diseño de Base de Datos****

* Define la estructura de almacenamiento de la información.
* Incluye la planificación de tablas, relaciones y consultas SQL.

**Proceso:**

* Identificación de datos clave en el proyecto.
* Creación de diagramas entidad-relación (ERD).
* Implementación y pruebas en entornos de desarrollo.

### ****5. Diseño de Backend****

* Planificación de la lógica de negocio y conexión con la base de datos.
* Desarrollo de APIs y estructuras de datos.

**Proceso:**

* Definición de requerimientos del backend.
* Creación de esquemas de rutas y controladores.
* Implementación de seguridad y pruebas de funcionalidad.

### ****6. Diseño de Frontend****

* Desarrollo de la interfaz del usuario en HTML, CSS y JavaScript.
* Integración con el backend y optimización del rendimiento.

**Proceso:**

* Creación de componentes reutilizables.
* Aplicación de frameworks (React, Vue, Angular).
* Pruebas de compatibilidad y accesibilidad.

Simulación Interactiva de Funcionalidad

Formato: Los equipos deben preparar una historia o escenario basado en un caso de uso típico que demuestre, cómo su módulo interactuaría con el usuario y con otros módulos del sistema.

Contenido dinámico:

**Escenario ficticio:** Crear un usuario ficticio y describir su interacción con la plataforma a través de su módulo. Por ejemplo, si es un módulo de asignación de aulas, simular cómo un profesor o administrador interactuaría con él, mostrando paso a paso qué vería en la interfaz y qué resultado recibiría.

Flujo interactivo: En lugar de una simple presentación, pueden utilizar herramientas como Google Slides, powton o Prezi para hacer la simulación más interactiva, permitiendo que los que estamos en clase, tomemos decisiones y seleccionemos opciones que afecten el flujo del caso de uso.

Cada grupo tendrá 15 minutos para exponer, divididos de la siguiente manera:

Ejemplo del Módulo de Autenticación

1. Introducción del Escenario y Usuario Ficticio (3 minutos)

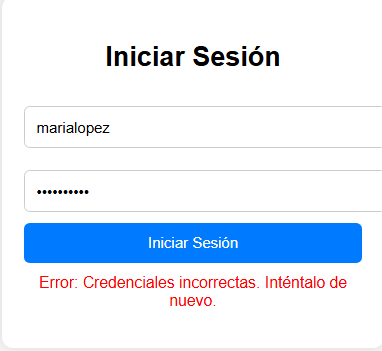
Usuario Ficticio: “María López”, administradora de la plataforma educativa.

Escenario: María necesita acceder al sistema de asignación de aulas para verificar las reservas de las próximas semanas. Antes de hacerlo, debe pasar por el módulo de autenticación que le solicitará sus credenciales.

Objetivo del Módulo: Garantizar que solo usuarios autorizados puedan acceder al sistema, asegurando la privacidad y seguridad de los datos.

Narrativa:

“María López, administradora académica, ha sido designada para gestionar las asignaciones de aulas. Para ello, primero debe iniciar sesión en el sistema utilizando sus credenciales. El módulo de autenticación valida su identidad mediante su nombre de usuario y contraseña. Si las credenciales son correctas, se le concede acceso; de lo contrario, recibe una notificación con el error.”



2. Demostración del Flujo de Uso del Módulo (6 minutos)

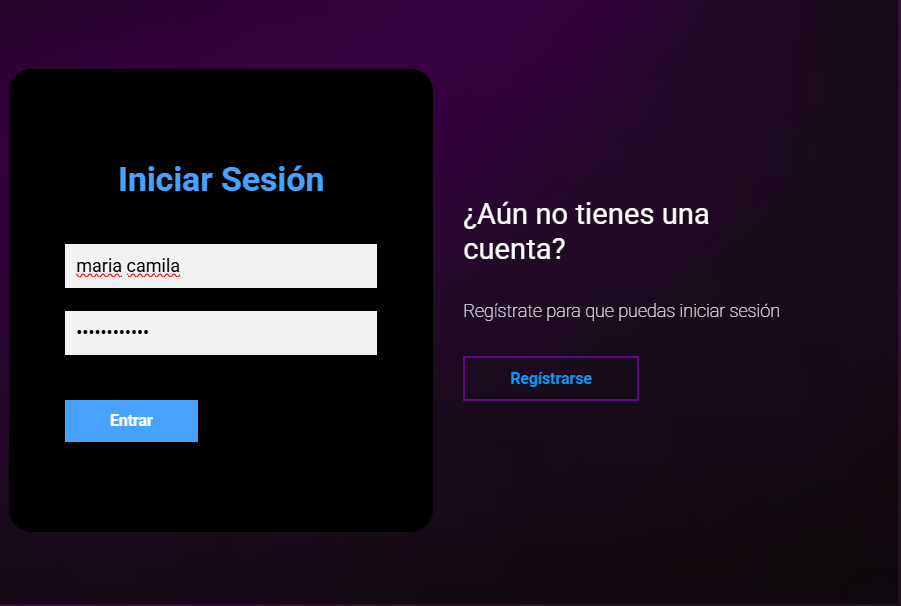
Flujo principal: Mostrar cómo María ingresa su nombre de usuario y contraseña en el formulario de autenticación.

Interacción con la interfaz:

María introduce su nombre de usuario: marialopez.

María introduce su contraseña: 12345secure.

Al hacer clic en "Iniciar Sesión", el sistema verifica sus credenciales.



Respuesta del sistema: El sistema devuelve un mensaje de éxito: “Autenticación exitosa. Bienvenida, María López” y redirige a la pantalla principal del sistema de asignación de aulas.

Interacción dinámica con la audiencia:

En este punto, el equipo puede pedir a la audiencia que elijan entre dos opciones:

Opción 1: Simular una autenticación correcta.

Opción 2: Mostrar qué sucede si hay un error (esto se cubrirá en el siguiente paso).

Herramienta visual: Prototipo en Figma o Google Slides que muestre la interacción paso a paso. Si el equipo ya tiene el sistema funcionando, pueden hacer una demo en vivo mostrando la pantalla del login y la respuesta del sistema.

3. Simulación de Errores o Excepciones (2 minutos)

Error 1: María introduce una contraseña incorrecta (123wrongpassword). El sistema detecta que la contraseña es inválida y muestra un mensaje: “Error: Contraseña incorrecta. Inténtalo de nuevo.”

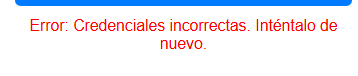
Error 2: María deja el campo de contraseña vacío. El sistema detecta que falta información y muestra el mensaje: “Error: Por favor, ingresa tu contraseña.”

Manejo de errores: Explicar cómo el sistema maneja estos errores, evitando que usuarios no autorizados accedan al sistema.

Narrativa:

“El módulo está diseñado para manejar errores comunes como contraseñas incorrectas o campos vacíos, brindando mensajes claros y sencillos que guían al usuario en la corrección de su error.”

Herramienta visual: Muestra de las diferentes pantallas o mensajes de error mediante simulaciones en Figma o presentaciones en Google Slides.



4. Explicación Técnica y Retos Superados (2 minutos)

Explicación Técnica:



El módulo de autenticación utiliza un sistema de hashing de contraseñas para asegurar que las credenciales no se almacenen en texto plano.

Interacción con la base de datos: Las credenciales se comparan con los registros almacenados de manera segura en la base de datos, utilizando un algoritmo de hash como bcrypt.

Tecnologías usadas: El módulo está construido con Node.js en el back-end y MongoDB para almacenar los datos de usuario. La autenticación se maneja mediante tokens JWT (JSON Web Tokens) para mantener la sesión de los usuarios activa.

Reto superado:

Problema: Inicialmente, la validación de contraseñas era lenta debido a la encriptación.

Solución: Optimizamos el proceso de autenticación utilizando un sistema de caché para validar contraseñas previamente verificadas de manera más rápida.

Herramienta visual: Un diagrama técnico simple en Lucidchart o Miro que muestre el flujo de autenticación, incluyendo la interacción con la base de datos y el uso de hashing.

5. Interacción Final con el Público y Preguntas (2 minutos)

Invitar preguntas:

“Ahora que han visto cómo funciona nuestro módulo de autenticación, ¿tienen alguna pregunta sobre su funcionamiento o su integración con el sistema de asignación de aulas?”

Interacción con la audiencia:

Puedes lanzar una pregunta a la audiencia: “¿Qué otros métodos de autenticación creen que podríamos agregar para mejorar la seguridad del sistema?” (Ejemplo: autenticación de dos factores).

1. **Autenticación de Dos Factores (2FA)**
   * Requiere un código adicional enviado por SMS, correo o una app como Google Authenticator.
   * Mejora la seguridad al agregar un paso extra además de la contraseña.
2. **Autenticación Multifactor (MFA)**
   * Combina **tres o más métodos de autenticación** (algo que sabes: contraseña, algo que tienes: token físico o app, algo que eres: huella digital o reconocimiento facial).
3. **Biometría (Reconocimiento Facial o Huella Digital)**
   * Usa datos biométricos para validar la identidad.
   * Más rápida y difícil de falsificar.
4. **Inicio de Sesión con Redes Sociales (OAuth 2.0)**
   * Permite iniciar sesión con cuentas de Google, Facebook, o Apple sin necesidad de una contraseña.
5. **Autenticación con Llaves de Seguridad (FIDO2)**
   * Uso de dispositivos físicos como **YubiKey** o autenticadores USB/NFC.
   * Muy seguro porque no requiere contraseñas.