Universidad Rafael Landívar
Facultad de ingeniería
Ingeniería en informática y sistemas
Estructuras de Datos II
Ing. Pablo Alejandro Godoy Díaz

PROYECTO DE APLICACIÓN

CHAT

Kevin Humberto Romero Villalta 1047519
José Vinicio De León Jiménez 1072619

Guatemala, 28 de noviembre del 2020

REQUERIMIENTOS DE SOFTWARE

Aplicación realizada en .Net Core:

Requerimientos mínimos:

- .NET SDK
  - .Net Core 3.1 o superior
  - MongoDB
  - IIS compiler
- Sistema Operativo:
  Sin requisito mínimo (Windows 7 o superior de preferencia)
- IDE:
  Visual Studio 2019

REQUERIMIENTOS DE HARDWARE

Requerimientos mínimos:

- Memoria RAM:
  500 MB
- Memoria en disco:
  Aproximadamente 124 MB de memoria en disco
- Procesador:
  Mínimo Pentium 2 a 266 MHz

ALCANCES EN LA FUNCIONALIDAD

- **MVC**

Se trata de una aplicación web bajo el patrón de diseño modelo, vista, controlador. En esta implementación de un chat se hace uso de una serie de vistas para que el usuario pueda consumir de manera intuitiva los servicios conectados a la api. En este proyecto también se incluyen las interfaces necesarias para la creación y autenticación de usuarios, luego de validarse las credenciales el usuario podrá observar su página principal única donde podrá iniciar una conversación segura con otro usuario registrado.

- **API**

En esta sección del proyecto se hizo uso de una aplicación de tipo API, en esta aplicación se llevan a cabo las conexiones con los algoritmos propios y con la base de datos no relacional MongoDB, para la transmisión de información entre proyectos se hace uso del estándar JSON, tanto para el manejo de usuarios como para el manejo de mensajes.

- **DLL**

En este archivo especial se encapsulan las clases utilizadas para encriptar y comprimir texto, específicamente se encuentran la clase de SDES, Diffie Hellman y LZW. Dichos algoritmos son utilizados en la API para cumplir con las funcionalidades necesarias de un chat seguro.

- **Consola**

La aplicación de consola fue utilizada para probar las funcionalidades por separado del proyecto sin necesidad de incurrir en el uso de la api, al ejecutar esta aplicación podrá visualizar el funcionamiento del proceso de generación de llaves y del proceso de descifrado de mensajes.

- **MongoDB**

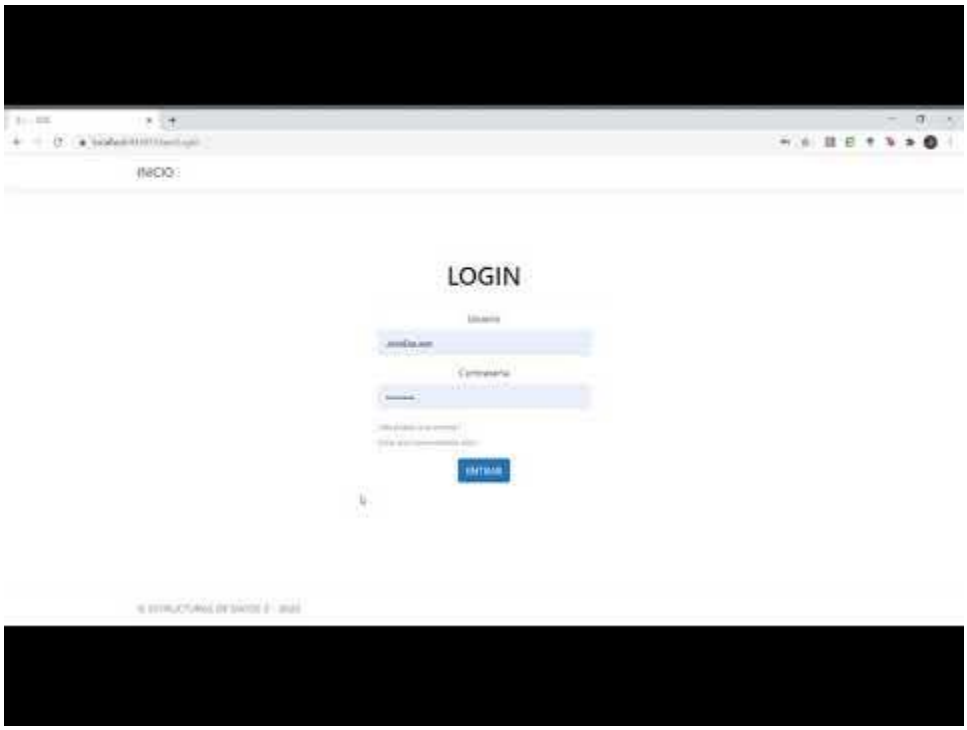
Esta base de datos no relacional fue utilizada para asegurar la persistencia de datos entre los usuarios registrados y los mensajes enviados entre estos, cabe mencionar que el contenido de los mensajes se cifra a través de los algoritmos descritos anteriormente en su interacción con la api.

ALGORITMOS UTILIZADOS

- **SDES**
  Para la encriptación de mensajes entre usuarios, también para la encriptación de contraseñas almacenadas.
- **Diffie Hellman**
  Para la generación de llaves únicas comunes entre dos pares de usuarios.
- **LZW**
  Para la compresión de archivos adjuntos en los mensajes de los usuarios.

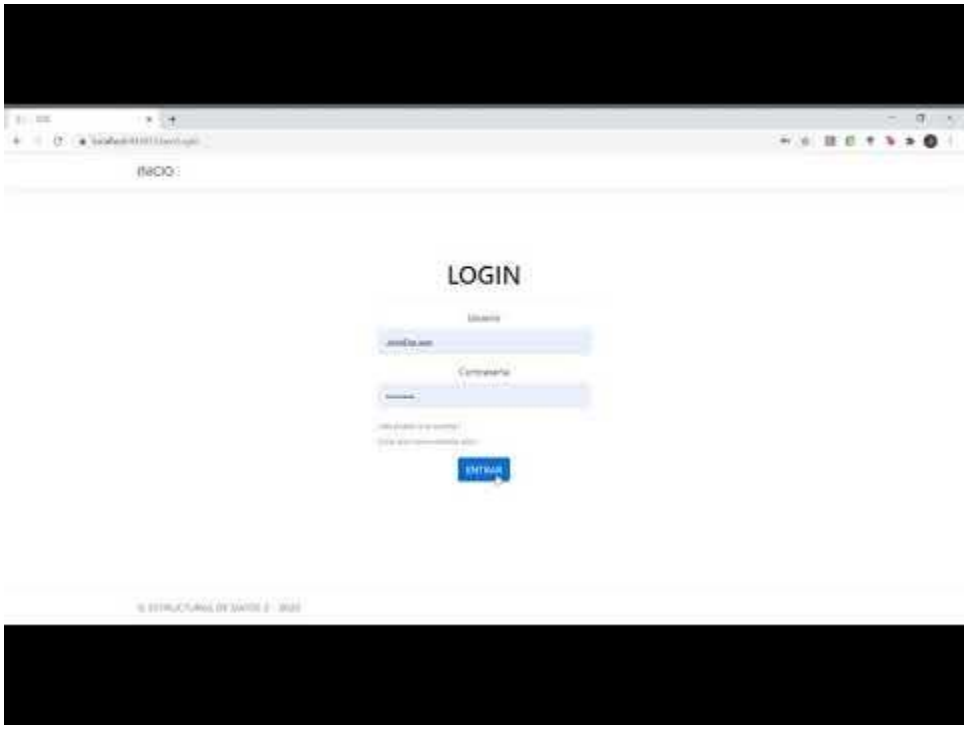
MANUAL DE USUARIO

- **Registro**



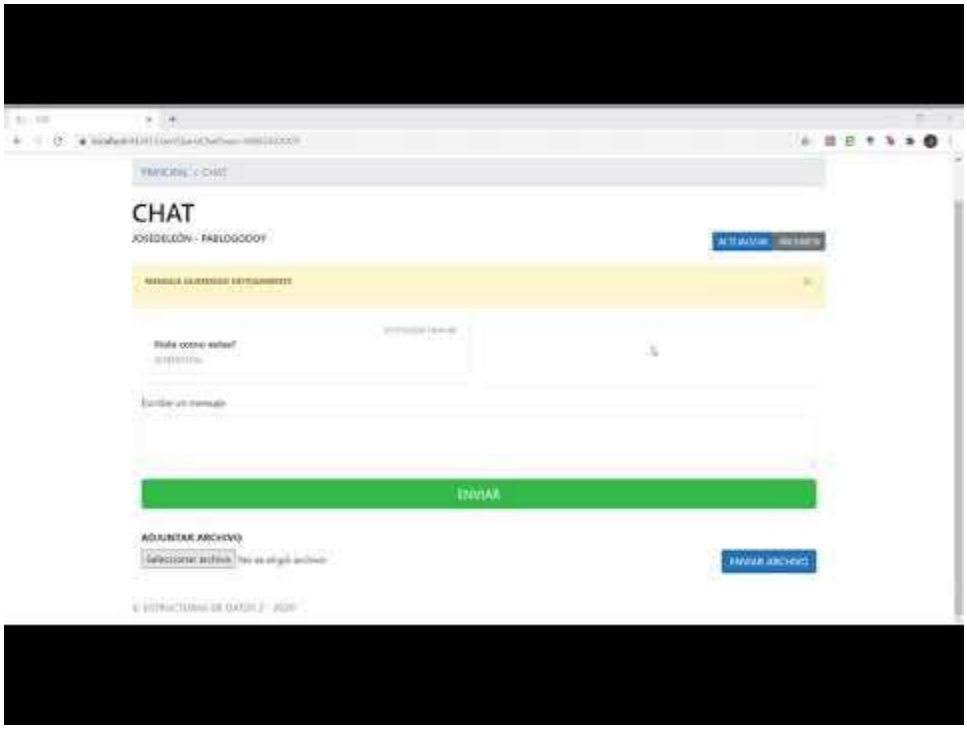
https://youtu.be/5MV3wRa5FG8

- **Login**



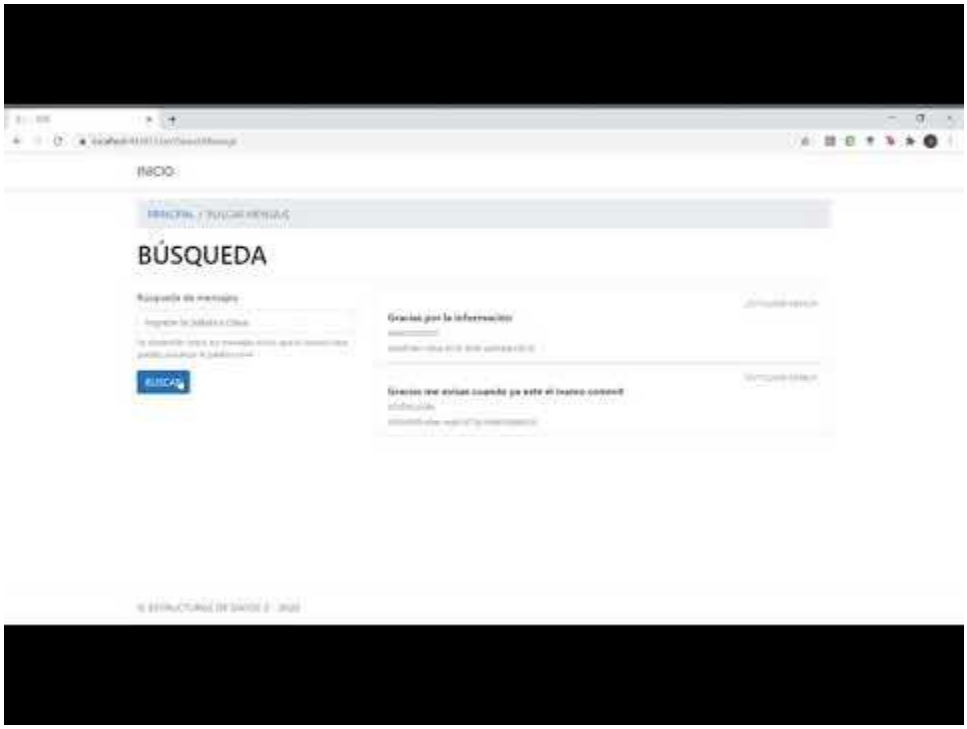
https://youtu.be/pnugYesmMOI

- **Chat**



https://youtu.be/2pD-Y-pEw-k

- **Búsqueda de mensajes**



https://youtu.be/LNJrgrpcGx8