**Control archivos**

**Universidad Tecnológica de Puebla**

**Tecnologías de la Información y Comunicación**

**Integrantes:**

**Adrian Ramos Carretero**

**Israel Sánchez Zamora**

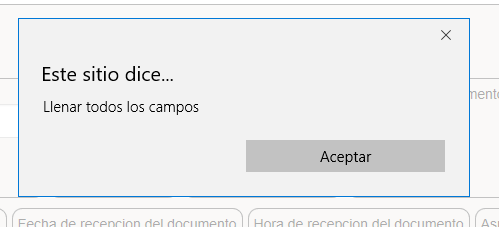
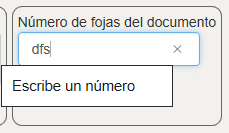
**Levy Argenis Velázquez Galindo**

**Javier Clavel Álvarez**

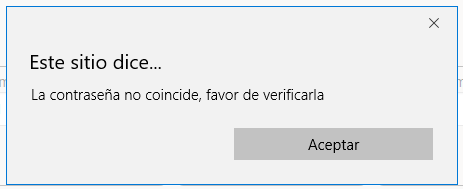
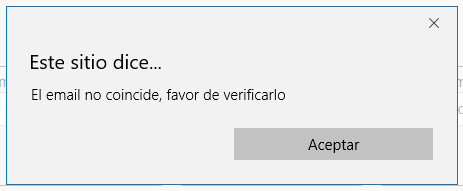
**Antonio Castell Camacho**

Validación tipo de datos en Formularios

En los formularios correspondientes a Usuario, Documento y Expediente, se realizaron las correspondientes validaciones de tipo de datos, es decir, si un valor es numérico, no aceptará ningún carácter, también verifica la estructura de email, el formato fecha y hora, además de validar que todos los campos se encuentren completados.



También se agregó una validación adicional en la entidad usuario para comparar el ingreso correcto del email y contraseña.



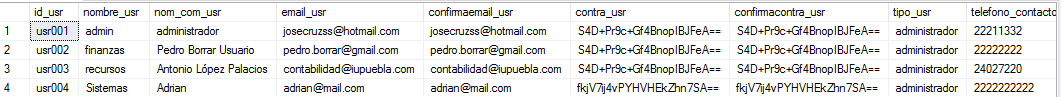
Encriptación

Se agrega la clase *“des\_encripta”*, misma que cumple dos funciones, encriptar datos y desencriptarlos.

Para realizar esta tarea elegimos el algoritmo de cifrado simétrico por bloques AES (Advanced Encription Standard o Estándar Criptográfico Avanzado), debido a que es un algoritmo muy completo, no vulnerable al criptoanálisis diferencial y lineal, además de que es necesaria una gran cantidad de textos encriptados y gran procesamiento para su análisis.

El algoritmo AES utiliza una de las tres fortalezas de clave de cifrado: una clave de encriptación (contraseña) de 128-, 192-, o 256- bits. Cada tamaño de la clave de cifrado hace que el algoritmo se comporte ligeramente diferente, por lo que el aumento de tamaño de clave no sólo ofrecen un mayor número de bits con el que se pueden cifrar los datos, sino también aumentar la complejidad del algoritmo de cifrado.

Para esta práctica se utilizó únicamente en la encriptación de la contraseña ingresada por el usuario.



A continuación se presenta parte del código implementado:

