

SISTEMA DE ENCRYPTACIÓN: PROTECCIÓN DE DATOS PERSONALES PARA CASA MONARCA

Axel Quiroga Caldera	A00832676
Diego Garza González	A01721186
Valeria María Serna Salazar	A01284960
Valeria Edith Lugo Gutiérrez	A00830523
Rubén Darío Castro Terrazas	A00833945

Gpo. 603

Miércoles 12 de junio de 2024

Escuela de Ingeniería y Ciencias

Profesores: Dr. Luis Miguel Meléndez Díaz y Dr. Daniel Otero

Instituto Tecnológico y de Estudios Superiores de Monterrey

Ingeniería en Ciencia de Datos y Matemáticas, Campus Monterrey

PROBLEMÁTICA

Casa Monarca da albergue a muchos migrantes, y junto con ellos toda su información personal, por lo que tiene importantes desafíos para cumplir su misión, entre los que destacan:

- Eficiencia a la hora de registrar nuevos ingresos.
- Asegurar la protección de los datos personales de cada migrante.
- Tener estadísticos en tiempo real sobre el estatus de la organización.



AES

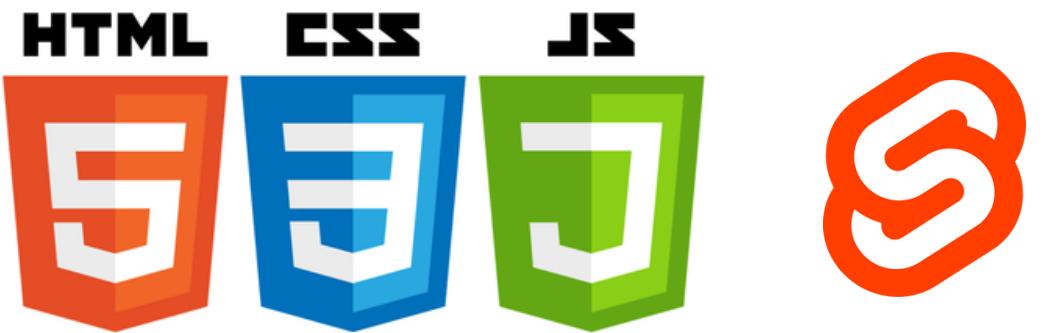
1. **Selección de Clave:** Se elige una clave de cifrado que puede ser de 128, 192 o **256 bits.**
2. **Preparación de Datos:** Los datos a cifrar (texto plano) se dividen en bloques de 128 bits. La clave se expande para generar varias subclaves mediante un algoritmo específico.
3. **Proceso de Cifrado:** Cada bloque pasa por procesos complicados que asegura seguridad.
4. **Rondas de Cifrado:** El proceso de cifrado se repite en varias rondas (**14 rondas** para una llave de 256 bits), aplicando las transformaciones anteriores y usando subclaves diferentes en cada ronda.
 - **Generación del Ciphertext:** Al finalizar todas las rondas, se obtiene el bloque cifrado final.

¿POR QUÉ AES?

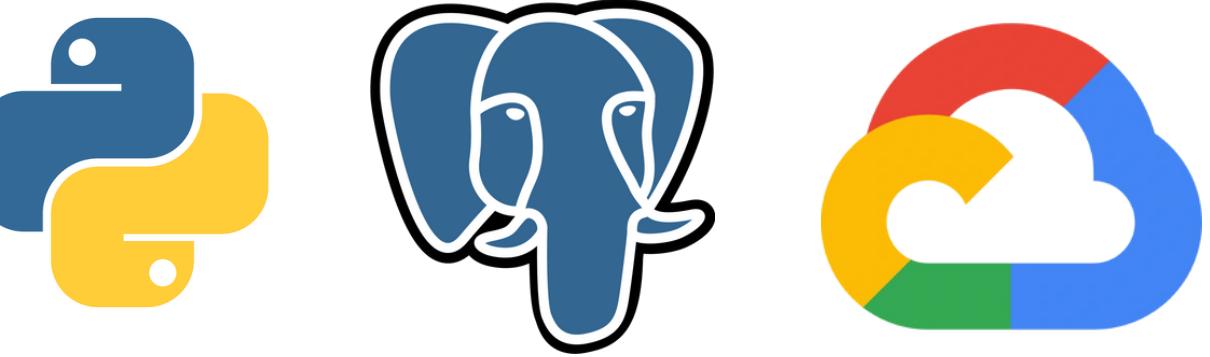
- **Seguridad:** Alta seguridad debido a su resistencia comprobada contra ataques criptográficos.
- **Rendimiento:** Rápido y eficiente en hardware y software.
- **Estándar:** Reconocido y adoptado globalmente como un estándar de cifrado (FIPS 197).
- **Versatilidad:** Soporta múltiples tamaños de clave (128, 192, 256 bits).
- **Fiabilidad:** Ha sido ampliamente analizado y probado por la comunidad criptográfica.

TECNOLOGÍAS UTILIZADAS

Front-End



Back-End



LOGIN, USUARIOS Y PERMISOS

Jerarquía de usuarios:

- **Usuario (Nivel 1):** Alta y buscar.
- **Servicios (Nivel 2):** Alta, buscar y servicios.
- **Administrador (Nivel 3):** Alta, buscar, servicios, reporte, cambiar estatus a inactivo, modificar permisos de usuarios.

FUNCIONAMIENTO GENERAL

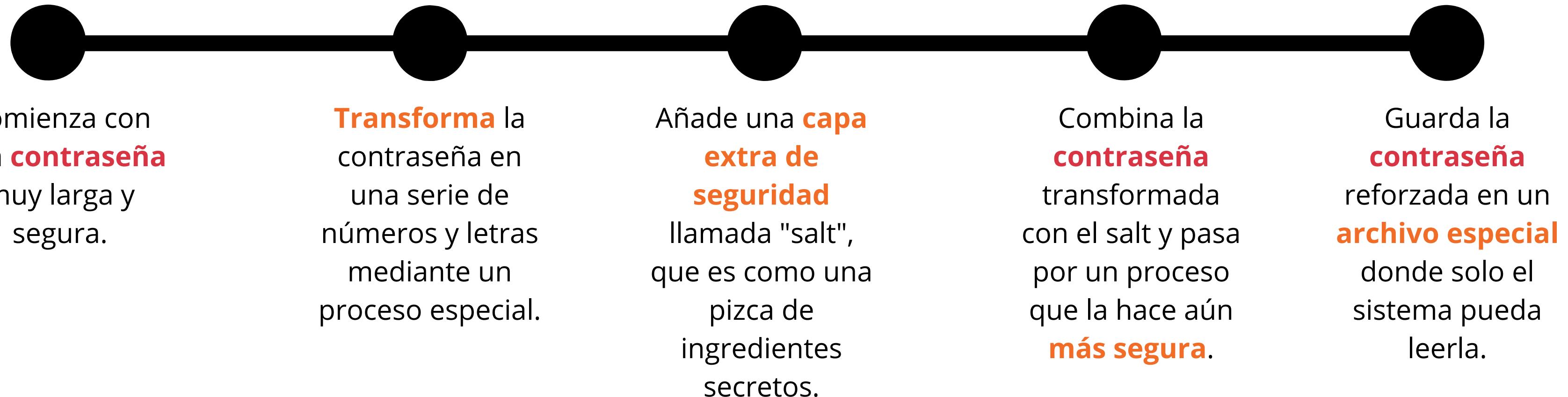
Para dar de alta:

1. El HTML recibe la respuesta a los cuestionarios.
2. Se encripta utilizando funciones en el backend de Python que fueron conectadas con un API.
3. Se envía a la base de datos encriptado. .

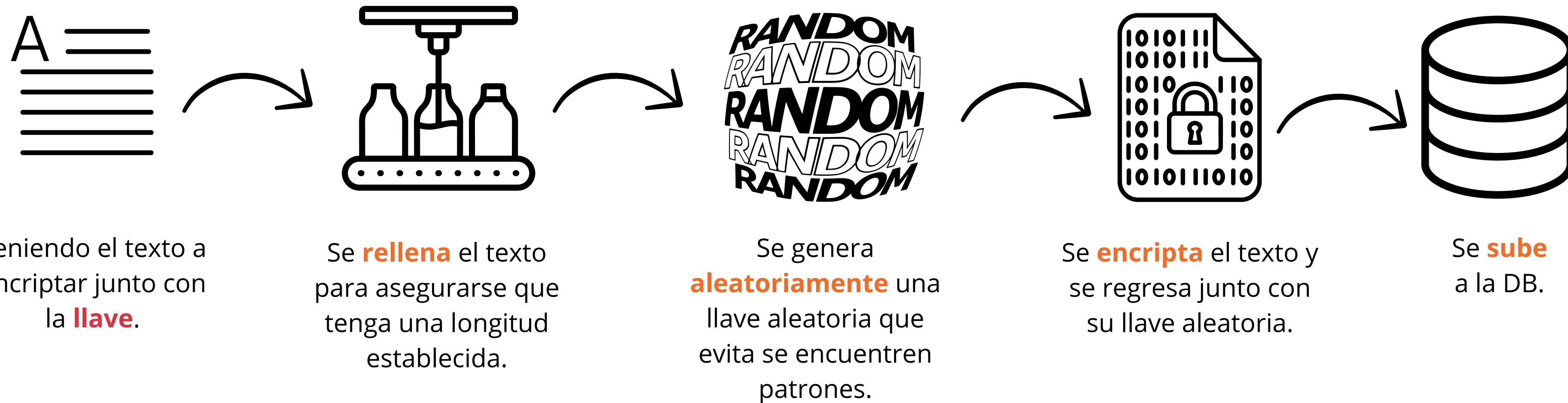
Para buscar o desplegar información:

1. Ingresa a la base de datos encriptada.
2. Se desencripta la información dentro del código.
3. Se busca al migrante específico.
4. Se despliega solo ese registro.

GENERACIÓN DE LA LLAVE



ALGORITMO - ENCRYPTACIÓN



ALGORITMO - DESENCRIPTACIÓN



CONEXIÓN A BASE DE DATOS

Se tienen 3 bases de datos en la nube:

migrantes

Registro inicial del Kobo.
73 columnas en total.

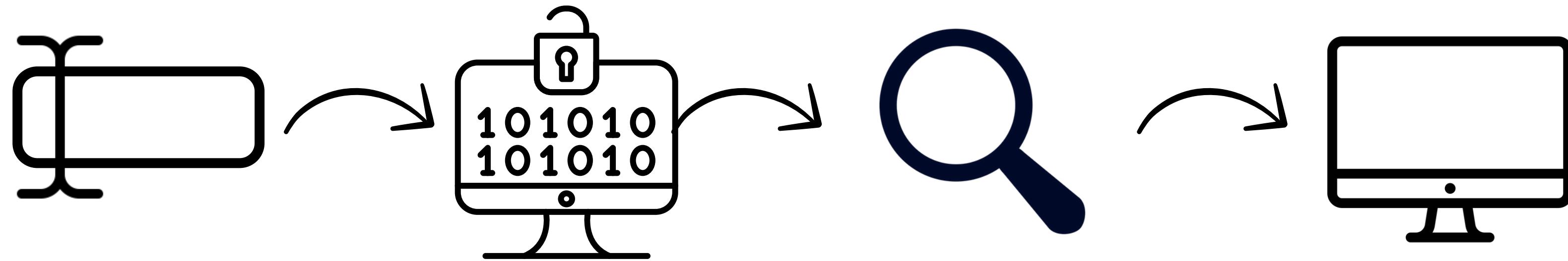
servicios

Se agregan servicios,
cada registro por servicio.
11 columnas en total.

ingresos

Cantidad de ingresos
por día.
7 columnas en total.

BUSCAR MIGRANTE



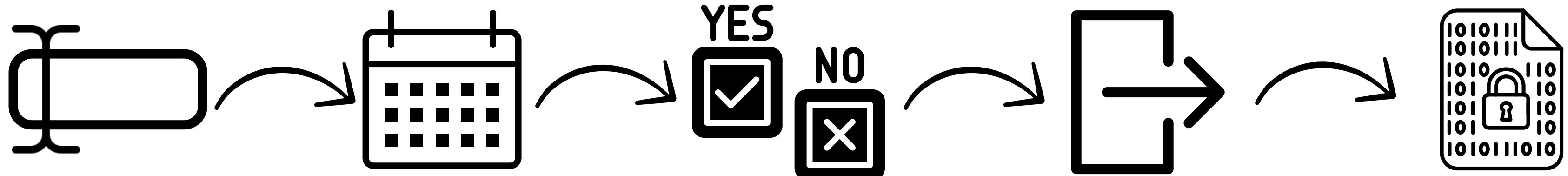
Búsqueda por nombre y fecha de nacimiento.

Se **extraen** los datos de la DB y se descriptan.

Uso de la **distancia Levenshtein** para encontrar migrante con el nombre más parecido.

Despliegue de datos, fotos y respuesta de formulario.

EDITAR ESTATUS A INACTIVO



Búsqueda por nombre y fecha de nacimiento.

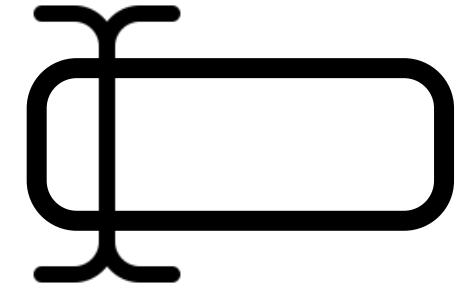
Ingresar la última fecha activo en casa monarca.

Se **modifica** la columna “activo_CM” de sí a no.

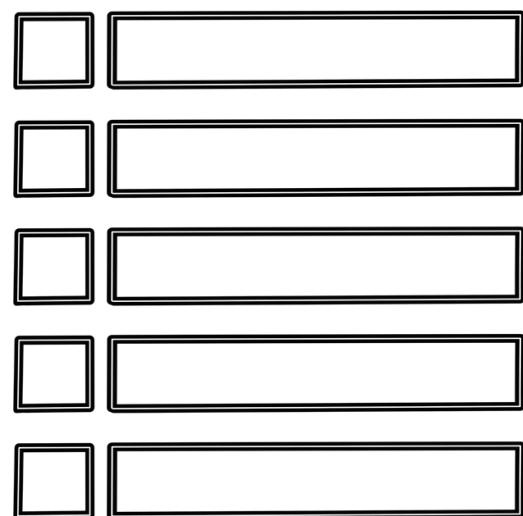
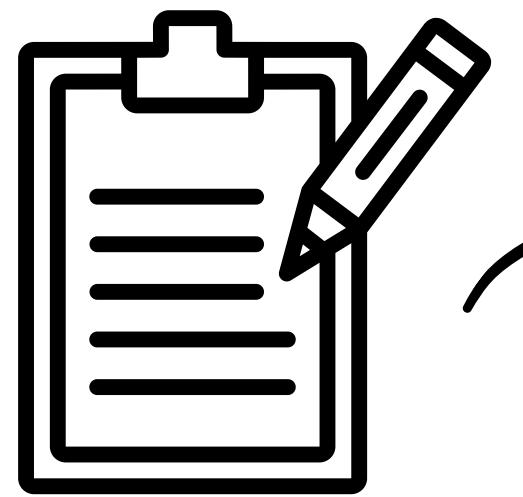
Se **agrega** la fecha de salida a la columna correspondiente.

Se **encriptan** los datos y se **actualizan** a la base de datos de migrantes.

AGREGAR SERVICIOS



Búsqueda por
nombre y fecha de
nacimiento.



- Inclusión
- Reubicación
- Educación
- Empleabilidad
- Salud mental

Llenado de formato
(checkbox).

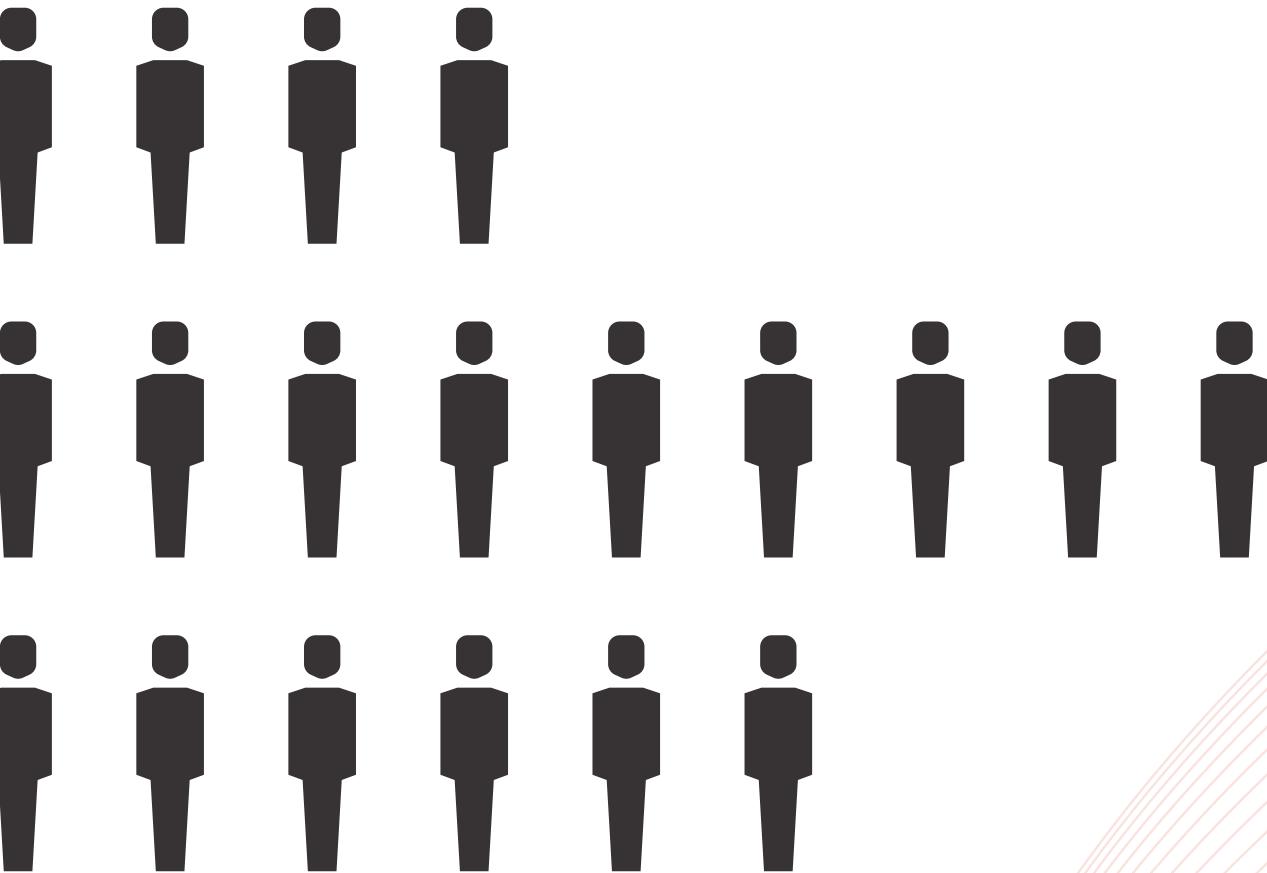
Datos se **encriptan**
y envían a la DB de
servicios.

CONTEO DE INGRESOS

Se realiza un conteo de los ingresos a casa monarca, considerando el tipo de población de son (Adulta/o, niña/o, etc) y la fecha de ingreso.

Esto se hace con la finalidad de poder llenar la información de fechas faltantes en la tabla de ingresos.

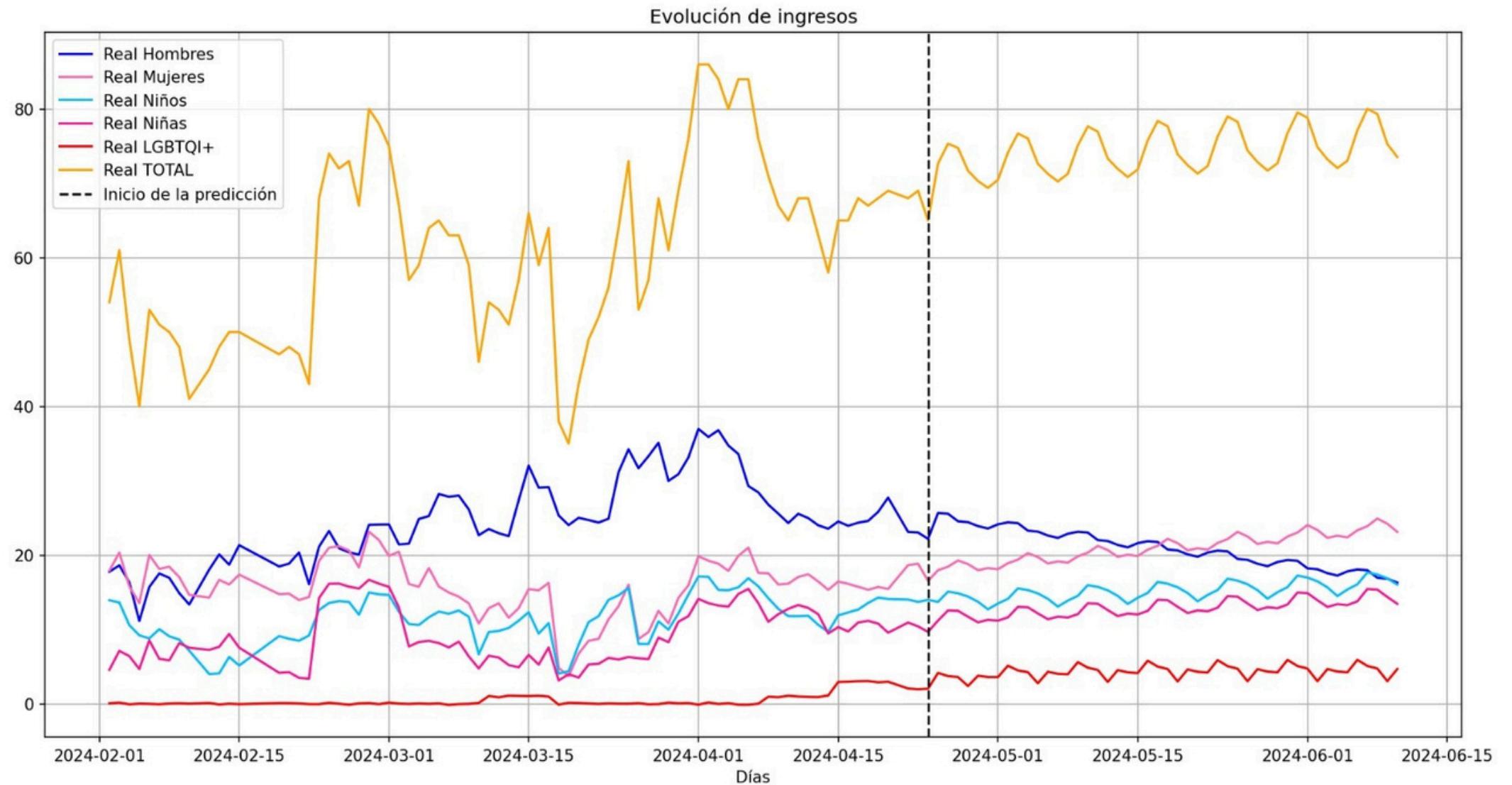
Con esta información, se puede planificar eficientemente la gestión de recursos y evaluar el estatus actual de Casa Monarca y sus migrantes, junto con realizar predicciones a futuro.



MODELO PREDICTIVO

Extrae los datos de “ingresos”, los desencripta y se le manda la cantidad a días a predecir.

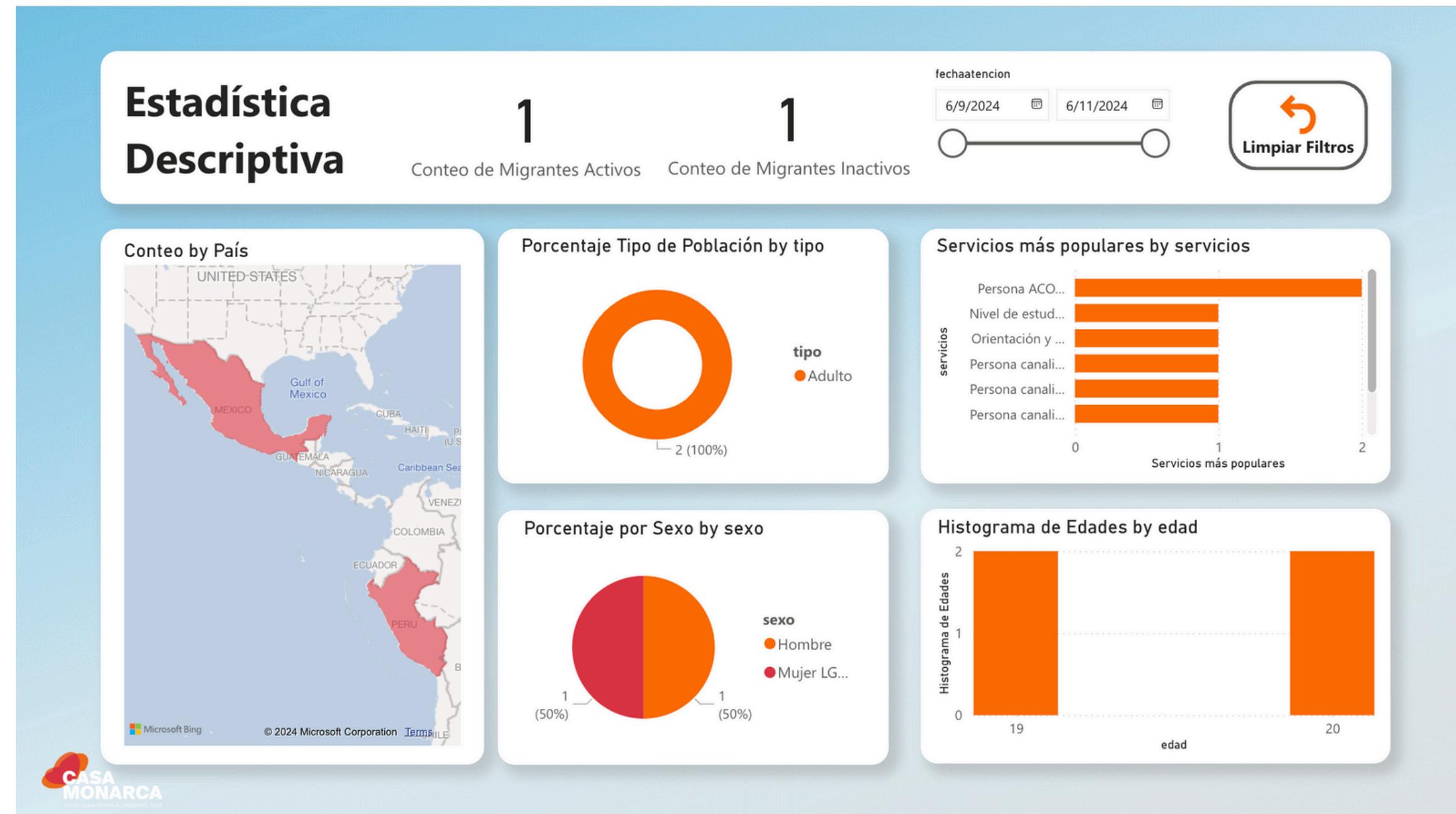
Con esos datos, se corre el modelo Prophet en Python y regresa una visualización de los ingresos estimados para cada categoría.



DASHBOARD

Desde PowerBI se conecta a la base de datos en la nube y a través de las funciones de Python desencripta los datos.

Una vez teniendo los datos, se crea el tablero.



DEMOSTRACIÓN



COSTOS DE USO

Concepto	Costo mensual
Costo por almacenamiento en SSD (250GB)	\$28.75 USD
Costo de respaldo para espacio adicional (+5% de incremento semanal)	\$4.75 USD
Costo por configuración de bajo costo (CPU mínima y almacenamiento necesario)	\$5.00 USD
Costo por copias de seguridad infrecuentes	\$3.00 USD
Costo por automatización de datos	\$2.00 USD
Total	\$43.50 USD

ÁREAS DE OPORTUNIDAD

- Al tener una base de datos en la nube en el plan gratuito, las consultas pueden llegar a tardar un par de segundos en cargar adecuadamente.
- Debido a la poca cantidad de datos en el modelo, la predicción no es tan certera como nos gustaría. Esto mejorará notoriamente conforme hayan más datos que entrenen correctamente al modelo.

VENTAJAS DE UTILIZAR LA PÁGINA

- Interfaz sencilla, fácil de utilizar.
- Seguridad garantizada al tener login y contraseña, con los permisos bien establecidos.
- Correcta encriptación y desencriptación de la información.
- Búsqueda de un migrante nuevo tomando en cuenta resultados similares, para evitar errores ortográficos al hacer la búsqueda.
- Capacidad de obtener estadísticas y predicciones en el momento deseado.