Universidad Politécnica de Chiapas.

Jesus Alberto Gonzalez Gutierrez

Arquitectura Orientada a Servicios

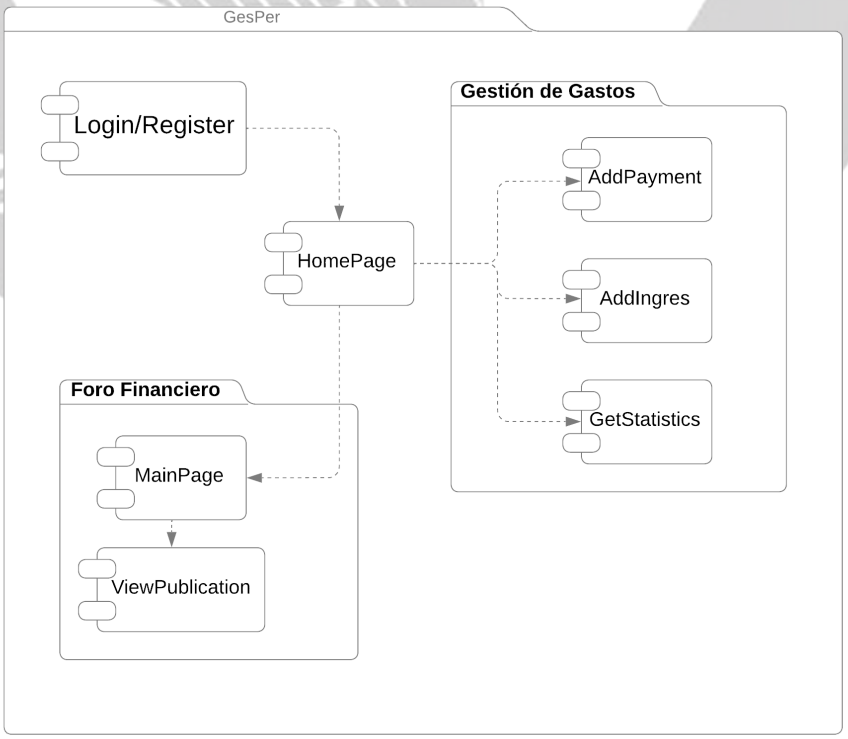
Corte 2

- Luis Daniel Molina Alfaro 201252
- Osvaldo Ángel Hernández 211125
- Arisel Fernández Cañaveral 211119

AOS.C2.A3 Avance de proyecto integrador

MSTG-ARCH-1 Identificación de componentes

1. **Pantalla de Inicio de Sesión y Registro:**
    a. Login: Una pantalla donde los usuarios pueden iniciar sesión en sus cuentas.
    b. Registration: Una pantalla para que los nuevos usuarios se registren en la aplicación.
2. **Pantalla Principal:**
    a. HomePage: La pantalla principal que muestra un resumen de gastos e ingresos, y proporciona acceso a otras funciones de la aplicación.
3. **Gestión de Gastos:**
    a. AddPayment: Una pantalla para agregar nuevos gastos así como su categoría y una descripción
    b. AddIngres: Una pantalla para agregar nuestros ingresos
    c. TransactionList: Una lista de transacciones que muestra los gastos e ingresos registrados por el usuario.
4. **Informes y Estadísticas:**
    a. GetStatistics: Una pantalla que muestra gráficos y estadísticas sobre los gastos e ingresos del usuario.
5. **Foro Financiero:**
    a. MainPage: Una sección donde los usuarios pueden postear sus dudas financieras
    b. ViewPublication: Una pantalla que muestra los detalles de una publicación y permite a los usuarios comentar en ella.



MSTG-ARCH-3 Se definió una arquitectura de alto nivel para la aplicación y los servicios y se incluyeron controles de seguridad en la misma

Dado que se trata de una aplicación desarrollada con Flutter, se ha optado por la arquitectura de software limpia para garantizar la eficiencia en el desarrollo y la implementación de las medidas de seguridad adecuadas.

Controles de Seguridad en la Arquitectura Bloc:

1. **Gestión de Sesiones y Autenticación:** Lo que permite aplicar controles de seguridad sólidos en la autenticación y la autorización de usuarios.
2. **Gestión de Errores y Excepciones:** Lo que es esencial para garantizar que la aplicación no exponga información sensible en caso de fallos.
3. **Seguridad en el Almacenamiento de Datos:** Aplicar técnicas de seguridad en el almacenamiento y la recuperación de datos en la base de datos, asegurando que los datos sensibles se cifren adecuadamente.
4. **Controles de Acceso:** Para garantizar que los usuarios solo tengan acceso a funciones y datos autorizados.

MSTG-ARCH-4 Se identificó claramente la información considerada sensible en el contexto de la aplicación móvil

1. **Contenido del Foro Financiero:**
    - Publicaciones y comentarios de los usuarios en el foro
        i. Información personal compartida en foro(nombre, dirección, etc.)
    - Información de la cuenta del usuario
2. **Tokens y Autenticación:**
    - Tokens de acceso utilizados en el proceso de autenticación
    - Usuario y contraseña de acceso
3. **Información del Administrador de Gastos**
    - Información de los gastos, ingresos y egresos del usuario

ID.AM-1: Se inventarian dispositivos y sistemas físicos dentro de la organización

Inventario de dispositivos

1. equipo de trabajo 01

   a. propiedad: Arisel Fernández Cañaveral
   b. tipo: laptop
   c. aditamentos extra:
      i. Monitor
      ii. Teclado
      iii. Mouse
2. equipo de trabajo 02
   a. propiedad: Osvaldo Ángel Hernández
   b. tipo: laptop
   c. aditamentos extra:
      i. 2 Monitores
      ii. Mouse
      iii. Teclado
3. equipo de trabajo 03
   a. propiedad: Luis Daniel Molina Alfaro
   b. tipo: Laptop
   c. aditamentos extra:
      i. Monitor
      ii. Teclado
      iii. Mouse
4. equipo de pruebas 01
   a. propiedad: Osvaldo Ángel Hernández
   b. tipo: teléfono inteligente
   c. aditamentos extra: ninguno
5. equipo de pruebas 02
   a. propiedad: Arisel Fernández Cañaveral
   b. tipo: teléfono inteligente
   c. aditamentos extra: ninguno

ID.AM-2: Se inventarian plataformas de software y aplicaciones dentro de la organización

Inventario de aplicaciones

1. **Visual Studio Code (VSCode)**:
   a. Windows: 1.63.2.
   b. Linux: 1.63.2.
2. **Android Studio**:
   a. Windows: 4.2.2.
   b. Linux: 4.2.2.
3. **PostgreSQL**:
   a. Windows: 13.2.
   b. Linux: 13.2.
4. **Postman**:
   a. Windows: 8.4.0.
   b. Linux: 8.4.0.

inventario de plataformas de software

1. Instancia de ec2 aws
2. Instancia de rds aws
3. Instancia de elastic load balancer aws
4. Instancia de base de datos en firebase(imágenes)
5. Figma

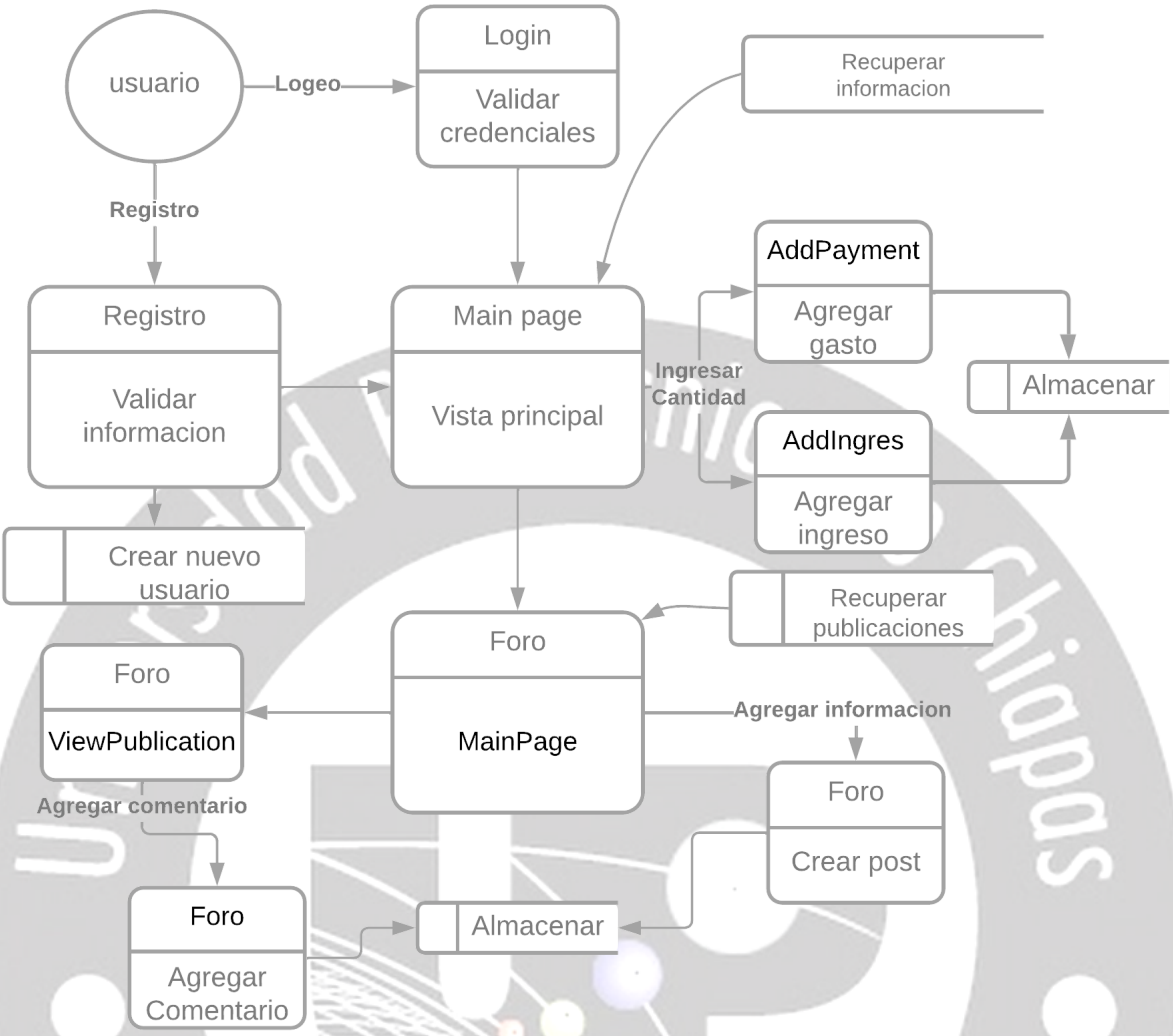
ID.AM-3: La comunicación organizacional y los flujos de datos se mapean

Comunicación Organizacional:

1. **Usuarios y la Aplicación:**
   - Los usuarios interactúan con la aplicación a través de las interfaces de usuario, como las pantallas de inicio de sesión, la pantalla principal, el registro de transacciones y el foro financiero.
2. **Comunicación entre Usuarios:**
   - Los usuarios pueden comunicarse a través del foro financiero, donde pueden crear publicaciones y comentar en las publicaciones de otros usuarios.

Flujos de Datos:

1. **Autenticación y Autorización:**
   - Cuando un usuario intenta iniciar sesión, la aplicación verifica las credenciales en el servidor.
2. **Gestión de Usuarios:**
   - Los datos de los usuarios, como la información personal, se almacenan en la base de datos.
   - La comunicación entre los usuarios y el servidor se utiliza para registrar nuevas cuentas de usuario y gestionar perfiles.
3. **Registro de Transacciones:**
   - Los datos de transacciones financieras se envían al servidor y se almacenan en la base de datos.
   - La aplicación muestra a los usuarios un resumen de sus transacciones financieras y estadísticas.
4. **Foro Financiero:**
   - Los usuarios pueden crear publicaciones y comentarios en el foro, lo que implica la comunicación entre usuarios y el servidor.
   - Los datos del foro se almacenan en la base de datos y se pueden acceder y modificar a través de la aplicación.



ID.AM-4: Los sistemas de información externos están catalogados

6. Instancia de ec2 aws
7. Instancia de rds aws
8. Instancia de elastic load balancer aws
9. Instancia de base de datos en firebase(imágenes)
10. Figma

ID.AM-6 Se establecen roles y responsabilidades de ciberseguridad para toda la fuerza laboral y los terceros interesados (por ejemplo, proveedores, clientes, socios)

Roles y Responsabilidades de Ciberseguridad:

- **Responsable de Seguridad (Project Manager):**
  - **Encargado:**
    - Luis Daniel Molina Alfaro

    - **Definición de Políticas de Seguridad:** Definir las políticas y los procedimientos de seguridad que se aplicarán en la aplicación
    - **Gestión de Incidentes de Seguridad:** Supervisa la respuesta a problemas de seguridad y coordina las medidas de resolución de problemas.

- **Desarrolladores:**
    - **Encargados:**
        - Osvaldo Ángel Hernández
        - Arisel Fernández Cañaveral
    - **Implementación de Seguridad:**Implementar las medidas de seguridad en la aplicación, como la autenticación, la validación de datos y el cifrado de datos.
    - **Pruebas de Seguridad:** Realizan pruebas de seguridad y corregirlos errores en caso de fallar las pruebas
    - **Actualizaciones de Seguridad:** Mantienen la aplicación actualizada con parches y actualizaciones de seguridad

ID.RA-1: Las vulnerabilidades de los activos se identifican y documentan

Los activos identificados son los siguientes:

- **Instancias de aws**
- **Instancia de Firebase**
- **Equipos de trabajo**
- **Equipos de prueba**
- **Fuerza laboral**

ID.RA-2: La inteligencia sobre amenazas cibernéticas se recibe de foros y fuentes de intercambio de información

No aplica: Esto debido a que no hay información de que existan amenazas cibernéticas o no se haya obtenido alguna retroalimentación/información de foros o fuentes externas

ID.RA-3: Las amenazas, tanto internas como externas, se identifican y documentan

No se han identificado amenazas externas o internas al momento de la realización de este documento

ID.RA-4: Se identifican los posibles impactos en el negocio y las probabilidades

No se han identificado ningún impacto en el negocio al momento de la realización de este documento

ID.RA-5: Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo

Al combinar la información de las amenazas identificadas previamente tanto como en el apartado MSTG-ARCH-6, las vulnerabilidades documentadas, las probabilidades y los impactos en el negocio, se calcula que el riesgo de un ataque, falló y/o impacto es moderadamente bajo. Por lo cual no se plantea implementar medidas adicionales para disminuir el riesgo ya que en caso de ocurrir, teóricamente, no afectará con significancia.

ID.RA-6: Las Respuestas a los riesgos se identifican y priorizan

- Falta de conocimientos en el uso de las tecnologías por parte del desarrollador
  - Capacitar previamente a los desarrolladores en las tecnologías a utilizar
  - Replantear los tiempos de entrega en base a la curva de aprendizaje durante el desarrollo
- Fallo en instancias de aws
  - Tener múltiples instancias de respaldo
  - Utilizar otros sistemas en la nube como respaldo en caso de una caída del sistema
- Robo o extravío de equipo de trabajo del desarrollador
  - Tener equipos de respaldo en caso de robo o extravío
  - Asegurar los equipos de trabajo después de la jornada laboral
- Pérdida de los archivos del proyecto por defectos en el equipo o intencionalmente hecho por el desarrollador
  - Mantener múltiples copias de seguridad en la nube
  - Limitar el acceso al manejo de los repositorios al personal no esencial
- Deserción por parte del equipo de trabajo
  - Proporcionar apoyo a los desarrolladores para que no se planteen el abandonar la carrera y/o el proyecto
- Problemas con la red eléctrica local y/o wifi
  - Contar con un sitio alternativo para poder realizar las funciones de trabajo
- Falta de resultados debido a plazos de entrega irrisorios
  - Replantear tiempos de entrega para entregar resultados en recuperación y/o extraordinario
  - Llevar un seguimiento de los avances del proyecto por parte del equipo de trabajo

- No contar con equipos que cumplan con las características necesarias para ejecutar correctamente el programa a desarrollar
    - Evaluar las características necesarias en base a las tecnologías a utilizar para garantizar el correcto funcionamiento a la hora de realizar la entrega
    - Contar con equipo de gama alta para no preocuparnos

MSTG-ARCH-5 Todos los componentes de la aplicación están definidos en términos de la lógica de negocio o las funciones de seguridad que proveen.

1. Autenticación y Gestión de Usuarios:

- **Registro e Inicio de Sesión:** Los usuarios pueden registrarse en la aplicación mediante una dirección de correo.
- **Seguridad de contraseñas:** La aplicación aplica políticas de seguridad de contraseñas, como la longitud mínima y complejidad.

2. Gestión de Transacciones Financieras:

- **Registro de Transacciones:** Los usuarios pueden agregar, editar y eliminar transacciones financieras, especificando la cantidad, descripción y una categoría.
- **Categorías de Gastos:** Las transacciones se pueden categorizar en gastos o ingresos, y se pueden agrupar en categorías(ocio, vivienda, servicios, etc).
- **Cálculo de Saldo:** La aplicación calcula y muestra el saldo actual en función de las transacciones registradas.

3. Estadísticas y Análisis:

- **Generación de Informes:** Los usuarios pueden generar informes y gráficos que muestran sus gastos e ingresos a lo largo del tiempo.
- **Seguimiento de Gastos:** Los usuarios pueden ver resúmenes y detalles de sus gastos en diferentes categorías.

4. Foro Financiero:

- **Publicaciones y Comentarios:** Los usuarios pueden crear publicaciones y comentarios en un foro financiero para discutir temas acerca de finanzas

MSTG-AUTH-5 Existe una política de contraseñas y es aplicada en el servidor.

Política de Contraseñas:

1. **Longitud Mínima de Contraseña:** Se establece una longitud mínima para las contraseñas para garantizar que su seguridad
2. **Complejidad de contraseña:** Se requiere que las contraseñas incluyan una combinación de caracteres, como letras mayúsculas y minúsculas, números y caracteres especiales.
3. **Almacenamiento Seguro de Contraseñas:** Las contraseñas de los usuarios se almacenan de manera segura cifrado hash para protegerlas contra posibles interceptación de datos.
4. **Token de seguridad:**Se establece un token temporal para cada sesión garantizando aumentando así la dificultad para un acceso malicioso

Aplicación en el Servidor:

La política de contraseñas se aplica en el servidor de la siguiente manera:

- Cuando los usuarios se registran o cambian sus contraseñas, la aplicación verifica que cumplan con los criterios previamente mencionados antes de realizarse el registro exitoso
- Las contraseñas se almacenan en la base de datos de manera segura utilizando cifrado hash
- Cuando los usuarios intentan iniciar sesión, el servidor verifica que la contraseña ingresada coincida con la contraseña almacenada en la base de datos después de aplicar la misma función de hash
- Cuando los usuarios intentan iniciar sesión y este es exitoso se crea un token temporal el cual es necesario para realizar las distintas funciones de la aplicación

MSTG-ARCH-6 Se realizó un modelado de amenazas para la aplicación móvil y los servicios en el que se definieron las mismas y sus contramedidas.

Lista de riesgos identificados

- Falta de conocimientos en el uso de las tecnologías por parte del desarrollador

    - ○ Capacitar previamente a los desarrolladores en las tecnologías a utilizar
    - ○ Replantear los tiempos de entrega en base a la curva de aprendizaje durante el desarrollo
- ● Fallo en instancias de aws
    - ○ Tener múltiples instancias de respaldo
    - ○ Utilizar otros sistemas en la nube como respaldo en caso de una caída del sistema
- ● Robo o extravío de equipo de trabajo del desarrollador
    - ○ Tener equipos de respaldo en caso de robo o extravío
    - ○ Asegurar los equipos de trabajo después de la jornada laboral
- ● Pérdida de los archivos del proyecto por defectos en el equipo o intencionalmente hecho por el desarrollador
    - ○ Mantener múltiples copias de seguridad en la nube
    - ○ Limitar el acceso al manejo de los repositorios al personal no esencial
- ● Deserción por parte del equipo de trabajo
    - ○ Proporcionar apoyo a los desarrolladores para que no se planteen el abandonar la carrera y/o el proyecto
- ● Problemas con la red eléctrica local y/o wifi
    - ○ Contar con un sitio alternativo para poder realizar las funciones de trabajo
- ● Falta de resultados debido a plazos de entrega irrisorios
    - ○ Replantear tiempos de entrega para entregar resultados en recuperación y/o extraordinario
    - ○ Llevar un seguimiento de los avances del proyecto por parte del equipo de trabajo
- ● No contar con equipos que cumplan con las características necesarias para ejecutar correctamente el programa a desarrollar
    - ○ Evaluar las características necesarias en base a las tecnologías a utilizar para garantizar el correcto funcionamiento a la hora de realizar la entrega
    - ○ Contar con equipo de gama alta para no preocuparnos

Propuesta actualizada unificando las propuestas anteriores

Resumen de la propuesta: GesPer es una aplicación para el manejo de gastos personales que permite al usuario registrar sus ingresos y egresos, categorizarlos, visualizarlos en gráficos y obtener reportes personalizados. Además, GesPer Un foro dentro de la aplicación donde los usuarios pueden compartir consejos y recomendaciones en cuestiones financieras, para fomentar la participación de los usuarios se ofrecerá un sistema de puntuación interno que les dará acceso a medallas y reconocimientos para recompensar su participación.

Introducción.

El proyecto **GesPer (Gestión Personal)** tiene como objetivo ayudar a las personas a controlar sus gastos personales y mejorar su economía. La propuesta se basa en el desarrollo de una aplicación que permita a los usuarios registrar sus ingresos y egresos, categorizarlos, visualizarlos en gráficos y obtener reportes personalizados. Además, **GesPer** la creación de una comunidad que busque fomentar buenos hábitos financieros mediante el uso de foros, comentarios y publicaciones básicas.

Objetivos
Diseñar e implementar un aplicación móvil para la gestión gastos personales además de un foro interno donde los usuarios podrán compartir información y consejos para mejorar sus hábitos financieros

Específicos

- Diseñar el maquetado de la aplicación
- Diseñar, implementar y desplegar la base de datos para la app usando Postgres
- Diseñar e implementar la API con su conexión front end utilizando express y Postgres.
- Diseñar e implementar las vistas para la aplicación móvil
- Integrar los componentes.

Lista de actividades

Actividades para alcanzar el Objetivo 1

1. **Definición de requisitos y alcance del proyecto**: Establecer los objetivos específicos y los límites del proyecto.
2. **Investigación y selección de tecnologías**: Investigar las tecnologías disponibles y seleccionar Node.js y Flutter como lenguajes de desarrollo.
3. **Diseño de la arquitectura de la aplicación**: Definir la estructura y los componentes principales de la aplicación.

Actividades para alcanzar el Objetivo 2

4. **Implementación del registro de ingresos y egresos del usuario**: Desarrollar la funcionalidad para que los usuarios puedan registrar sus ingresos y egresos.

5. **Visualización del balance mensual, semanal o diario**: Crear gráficos y tablas para mostrar el balancefinanciero del usuario en diferentes períodos.
6. **Generación de reportes personalizados**: Desarrollar la funcionalidad para generar reportes personalizados basados en los datos registrados por el usuario.

Actividades para alcanzar el Objetivo 3

7. **Implementación del registro de usuarios y login del usuario**: Desarrollar la funcionalidad para que los usuarios puedan registrar sus cuentas e iniciar sesión.

8. **Implementación módulo de blog y comentarios**: Desarrollo del módulo de blog que contendrá publicaciones, editarlas, eliminarlas y su respectiva sección de comentarios.
9. **Implementación del módulo de recompensas**: Desarrollar la funcionalidad para que los usuarios generen una puntuación interna la cual les dará acceso a distintas medallas que puedes presumir en sus perfiles.

Actividades para alcanzar el Objetivo 4

10. **Pruebas y correcciones**: Realizar pruebas exhaustivas de la aplicación y corregir cualquier error o problema identificado.

Dosificación

1. **Semana 1**: Definición de requisitos y alcance del proyecto.

2. **Semana 2**: Investigación y selección de tecnologías.
3. **Semana 3**: Diseño de la arquitectura de la aplicación y correcciones.
4. **Semana 4-5**: Implementación del registro de ingresos y egresos.
5. **Semana 6-7**: Visualización del balance mensual, semanal o diario.
6. **Semana 8-9**: Generación de reportes personalizados.
7. **Semana 10-11**: Implementación del registro de usuarios y login del usuario
8. **Semana 12-13:** Implementación módulo de blog y

comentarios
9.**Semana 13-14:** Implementación del módulo de recompensas
10.**Semana 14-15**: Pruebas y correcciones.

Cómo encaja la propuesta en las materias de SOA, Programación para móviles y Seguridad.

Soa: En la materia de soa aprendemos a crear backend con arquitecturas limpias las cuales nos permiten tener un mejor orden, flujo de trabajo y entendimiento además de permitirnos separar los módulos en microservicios para así mejorar la escalabilidad de la app, su mantenimiento y desarrollo.

Programacion para moviles: Para poder llevar nuestras finanzas a todos lados hemos apostado por el formato móvil, así poder mantenernos actualizados en los temas de interés de los blogs en los que participamos y estar pendientes de nuestras alertas si estamos llegando a nuestro límite financiero

Seguridad: Debido a que en las cuentas de usuario se maneja la información de los ingresos de los usuarios es importante para nosotros mantenerla a salvo para evitar su uso malintencionado aplicando buenas prácticas para el manejo de la información