SEGURIDAD EN EL DESARROLLO

DE APLICACIONES

INFORMACIÓN INICIAL DEL MODELO DE AMENAZAS

Nombre de la aplicación: OcoTaxi
Versión de la aplicación: 1.0
Descripción: La aplicación móvil para el servicio de taxis es una primera versión o implementación para facilitar los procesos que conllevan tomar un taxi o bien buscar pasajeros. La aplicación brindará opciones para que los taxistas y los pasajeros puedan comunicarse para obtener/brindar el servicio. Al ser la primera versión de la aplicación, su funcionalidad será limitada y contará con los siguientes usuarios:

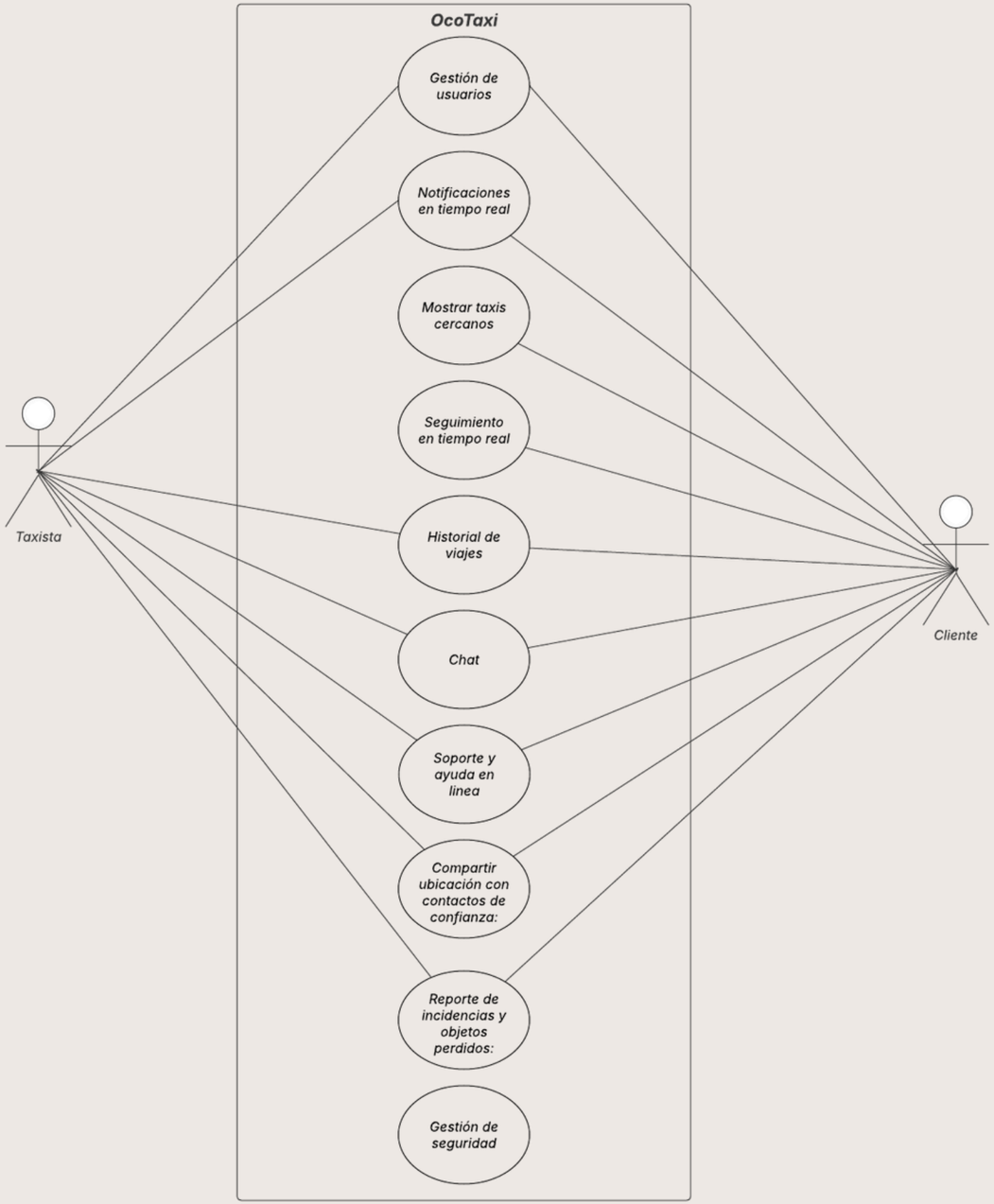
Taxistas
Clientes

Los taxistas y los clientes podrán tener una cuenta para iniciar sesión, los taxistas podrán brindar sus servicios en la aplicación y los clientes (pasajeros) podrán solicitar el servicio de taxi.

DEFINIR LOS REQUERIMIENTOS FUNCIONALES

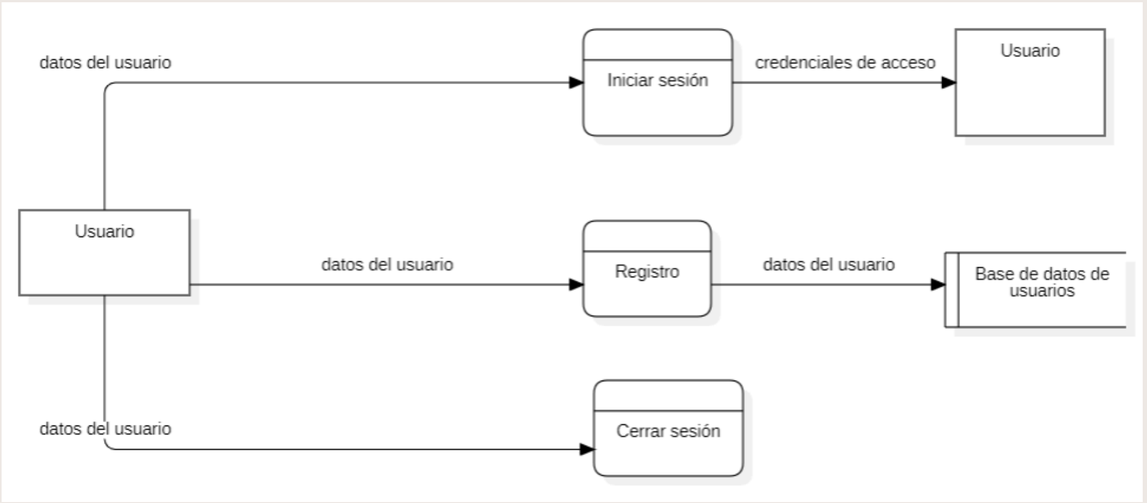
- Gestión de usuarios: la aplicación debe permitir a los usuarios interactuar con la aplicación, la cual debe incluir el registro, el inicio de sesión y la opción de cerrar sesión en cualquier momento.
- Mostrar taxis cercanos disponibles: la aplicación debe mostrar un mapa con los taxistas disponibles cercanos al cliente, el cliente podrá ver la información del taxista y solicitar el servicio
- Notificaciones en tiempo real: la aplicación debe notificar al taxista sobre las solicitudes que tiene, también debe notificar al cliente cuando su solicitud sea aceptada o rechazada
- Seguimiento en tiempo real: deber contar con seguimiento del taxi asignado cuando el cliente comience su viaje
- Elegir método de pago: el cliente podrá escoger el método de pago para cada viaje
- Historial de viajes: la aplicación debe recopilar la información sobre los viajes realizados (taxista / cliente) y tener un apartado para mostrárselo al usuario
- Chat entre el taxista y el cliente: debe contar con un sistema de chat para que el taxista y el cliente puedan interactuar
- Soporte y ayuda en línea: la aplicación debe contar con un foro para que los usuarios puedan obtener ayuda e información.
- Gestión de seguridad en la aplicación: la aplicación debe contar con seguridad suficiente para evitar pérdidas de información o errores dentro de ella.
- Panel de administración para el monitoreo y control de operaciones: la aplicación debe contar con un apartado de monitoreo que permita ver los detalles internos de la aplicación
- Reporte de incidencias y objetos perdidos: la aplicación debe contar con la opción de reportar objetos perdidos a los clientes que hayan ocupado el servicio
- Compartir ubicación y detalles con contactos de confianza: el usuario podrá compartir su ubicación e información del viaje con contactos de confianza

DIAGRAMA DE CASOS DE USO

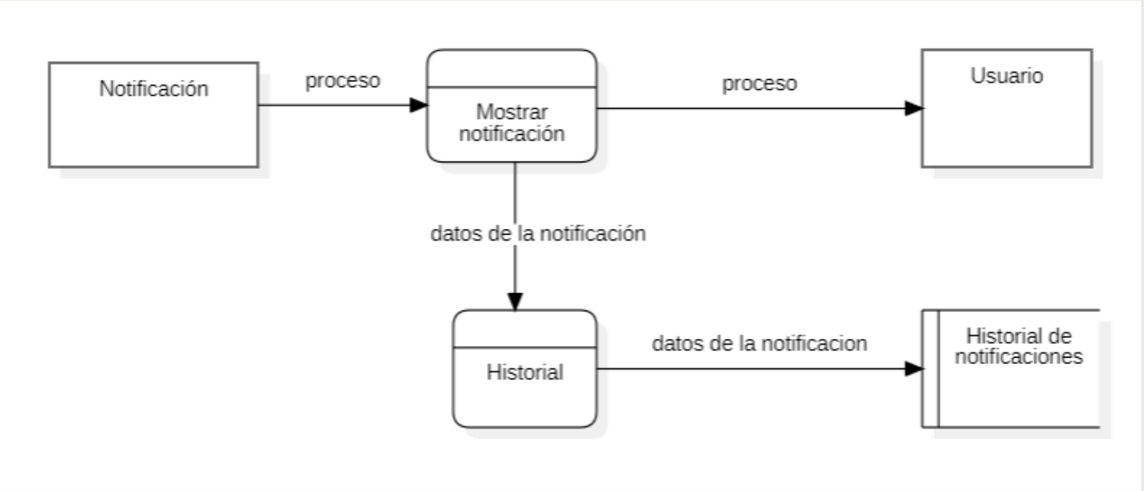


DIAGRAMAS DE FLUJO DE DATOS

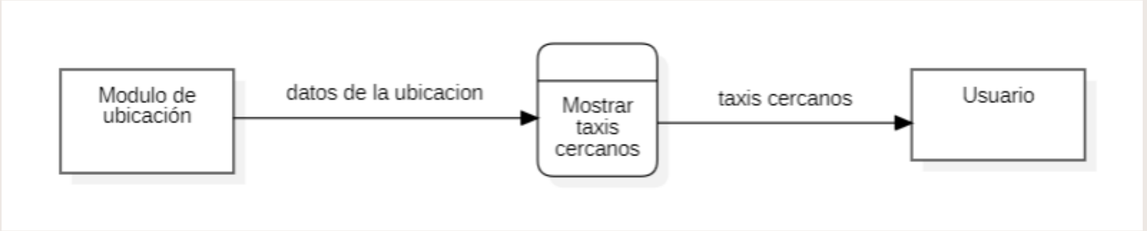
Gestión de usuarios



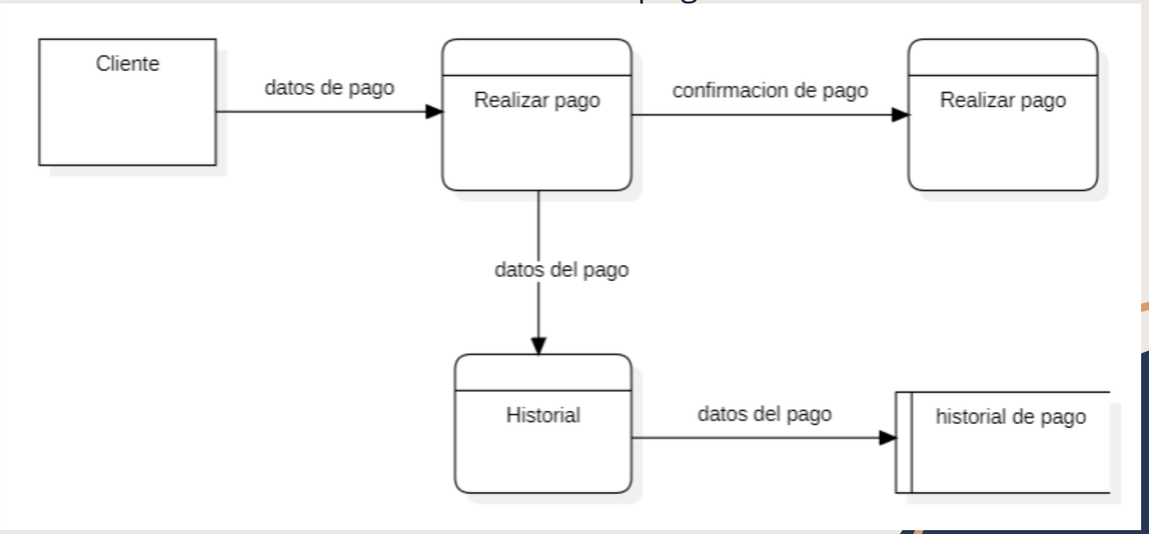
Notificación



Ver taxis cercanos

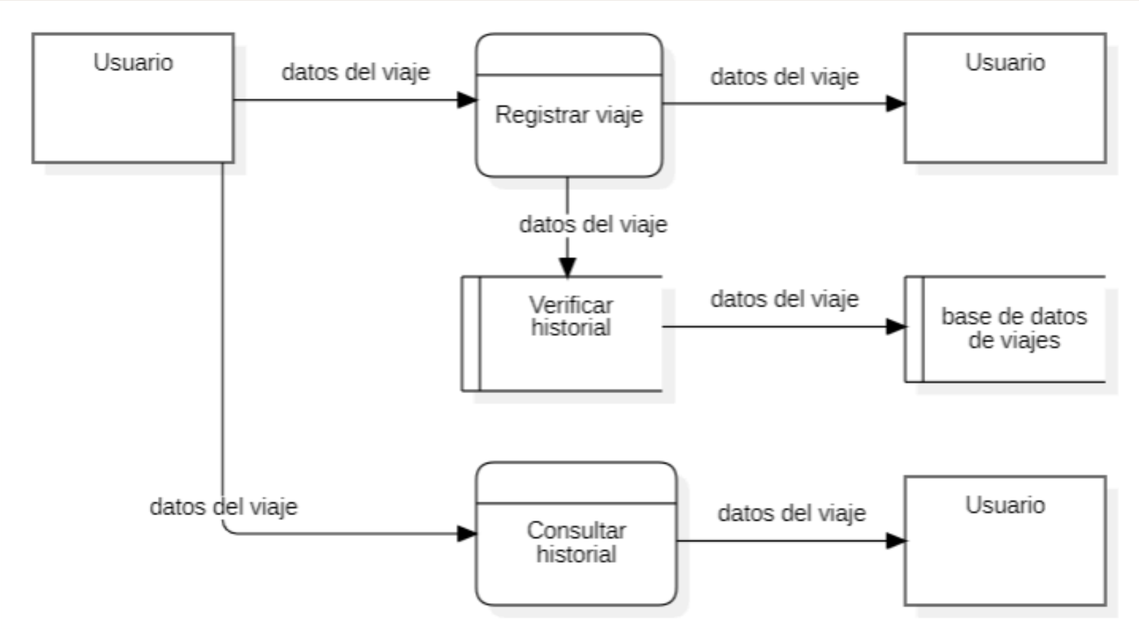


Métodos de pago

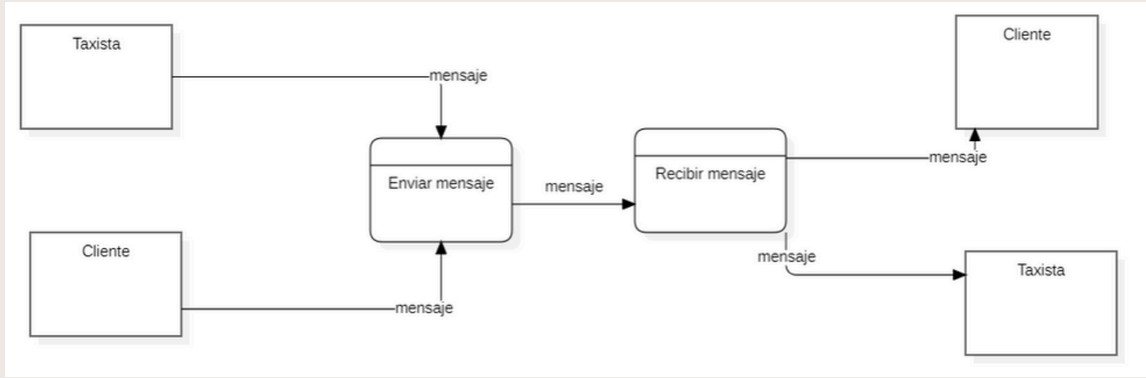


DIAGRAMAS DE FLUJO DE DATOS

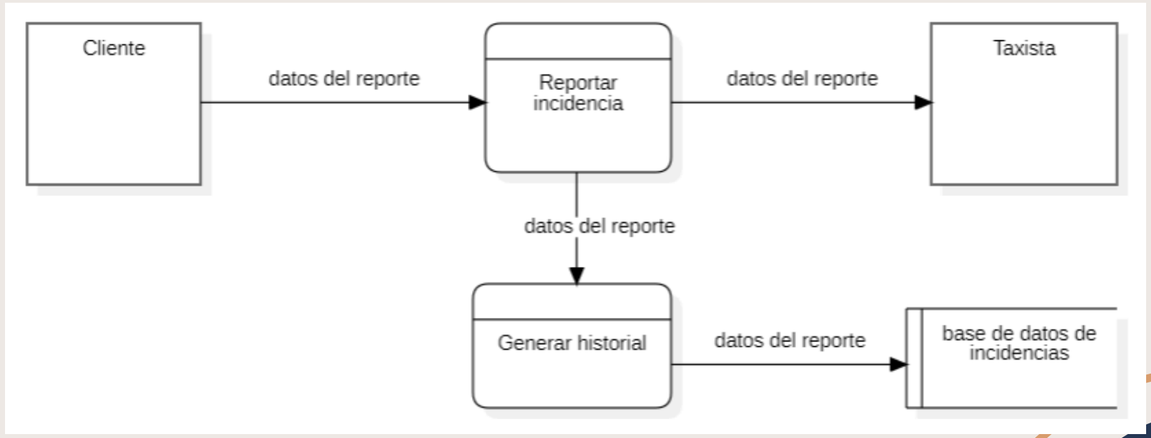
Historial de viaje



Chat

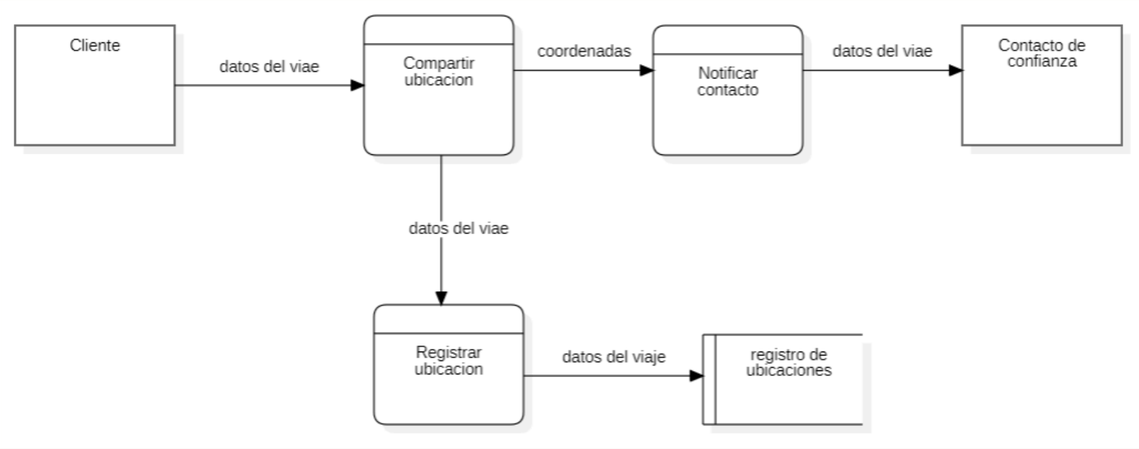


Reporte de incidencias

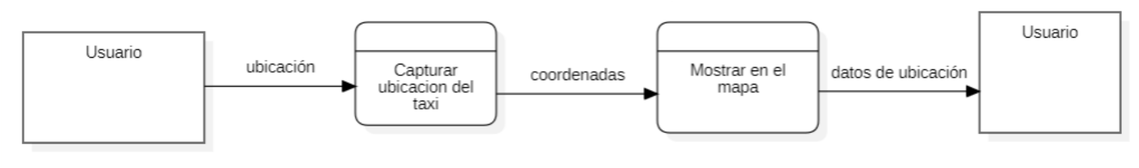


DIAGRAMAS DE FLUJO DE DATOS

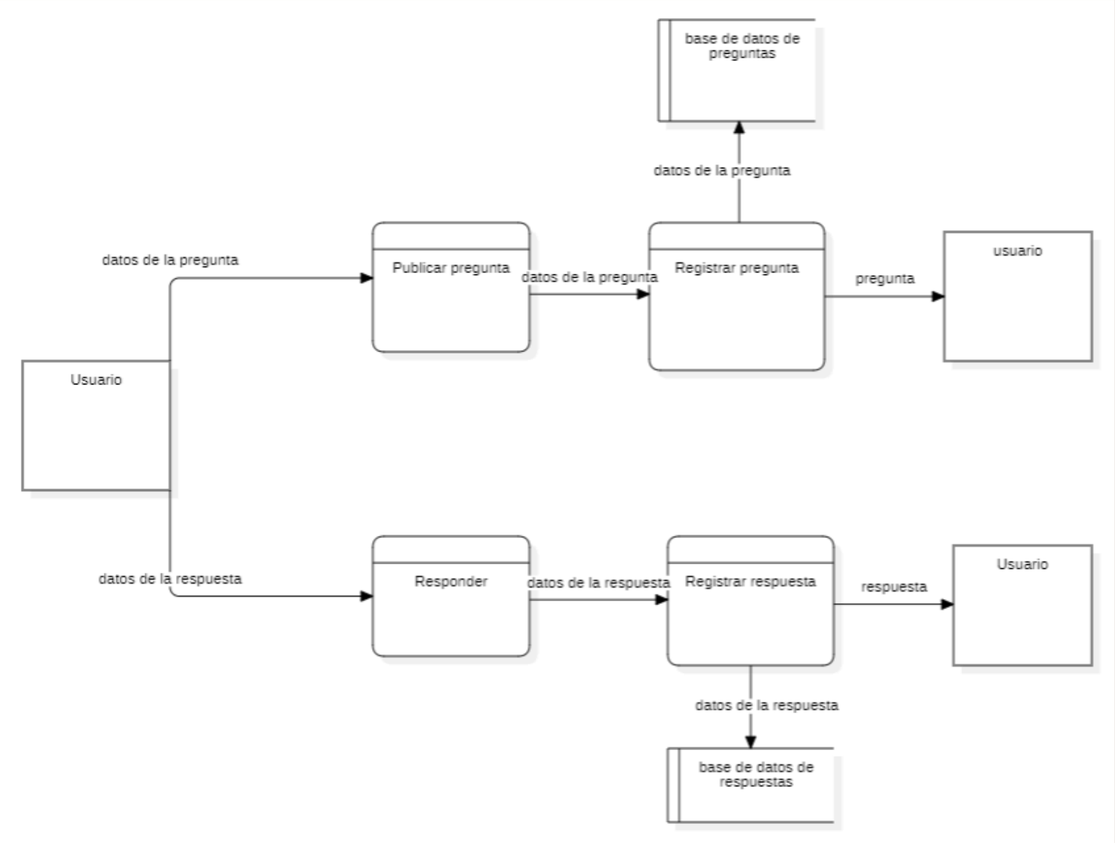
Compartir ubicación con contacto de confianza



Ubicación en tiempo real

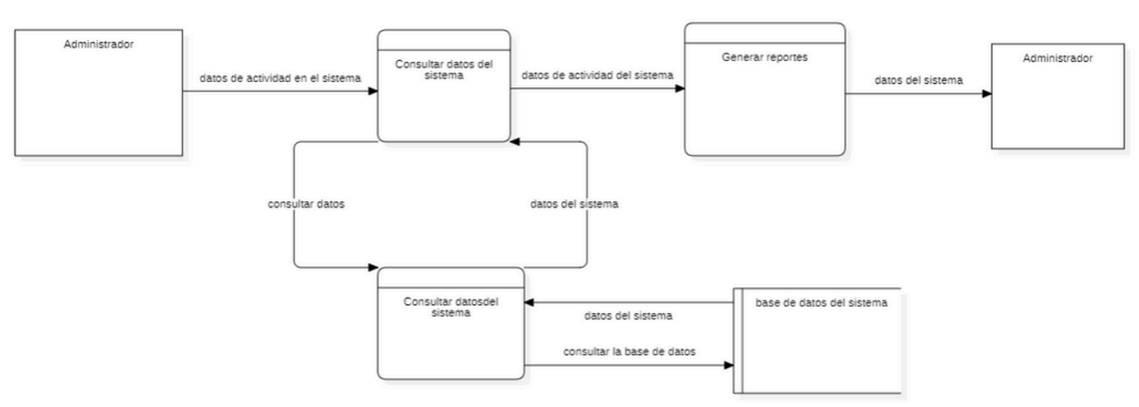


Foro

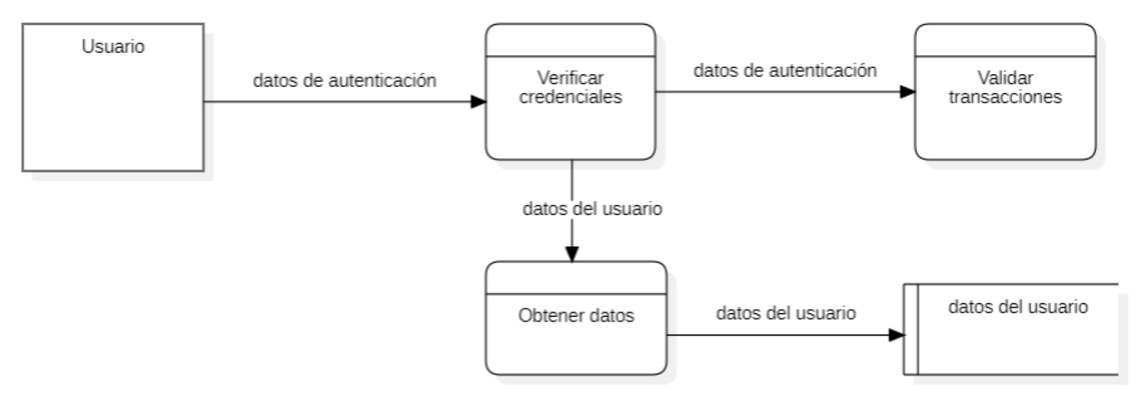


DIAGRAMAS DE FLUJO DE DATOS

Panel de administración



Seguridad de la aplicación



DEPENDENCIAS EXTERNAS DE LA APLICACIÓN

ID	Descripcion
1	Para gestionar notificaciones en tiempo real entre clientes y taxistas utilizaremos *Firebase Cloud Messaging (FCM)* o *OneSignal*
2	Para gestionar notificaciones en tiempo real entre clientes y taxistas utilizaremos Firebase Cloud Messaging (FCM) o OneSignal
3	Para permitir pagos electrónicos seguros dentro de la aplicación móvil se usará Stripe, PayPal o MercadoPago
4	Para autenticación de usuarios y verificación vía SMS o email se usará Twilio o Firebase Authentication
5	Para implementar el chat entre taxista y cliente en tiempo real dentro de la aplicación móvil usaremos Socket.io o Firebase Realtime Database
6	Para almacenar fotos de perfil, documentos y otros archivos en el caso de los taxistas dentro la aplicación web usaremos AWS S3 o Firebase Storage
7	Para gestionar la lógica de negocio, seguridad y almacenamiento de datos para ambas aplicaciones usaremos Backend en Laravel
8	Para almacenar información de usuarios, viajes, pagos e incidencias en ambas aplicaciones usaremos Base de datos MySQL

PUNTOS DE ENTRADA DE LA APLICACIÓN

ID	Nombre	Descripción	Niveles de confianza
1	Registro/Login	Permite el acceso y autenticación de usuarios	(1) Usuario anónimo (2) Usuario registrado
2	Registro de taxistas	Permite a los taxistas registrarse y enviar documentos para aprobación.	(1) Usuario anónimo, (4) Administrador
3	Solicitud de taxi	Punto de entrada para solicitar un servicio de taxi.	(2) Usuario registrado
4	Mapa de taxis disponibles	Punto de acceso al mapa en tiempo real.	(2) Usuario registrado
5	Chat	Punto de comunicación entre taxista y cliente.	(2) Usuario registrado
6	Reporte de incidencias	Permite a los usuarios enviar reportes.	(2) Usuario registrado
7	Panel de administración	Acceso al panel de control y monitoreo.	(4) Administrador
8	Gestión de tarifas y disponibilidad	Permite a los taxistas actualizar su disponibilidad y tarifas.	(3) Usuario registrado (Taxista)
9	Asignación de viajes	Permite a los taxistas aceptar o rechazar solicitudes de viaje.	(3) Usuario registrado (Taxista)
10	Centro de soporte	Punto de contacto para ayuda a clientes y taxistas.	(2) Usuario registrado, (4) Administrador
11	Sistema de calificaciones	Permite a clientes y taxistas evaluar la experiencia del viaje.	(2) Usuario registrado

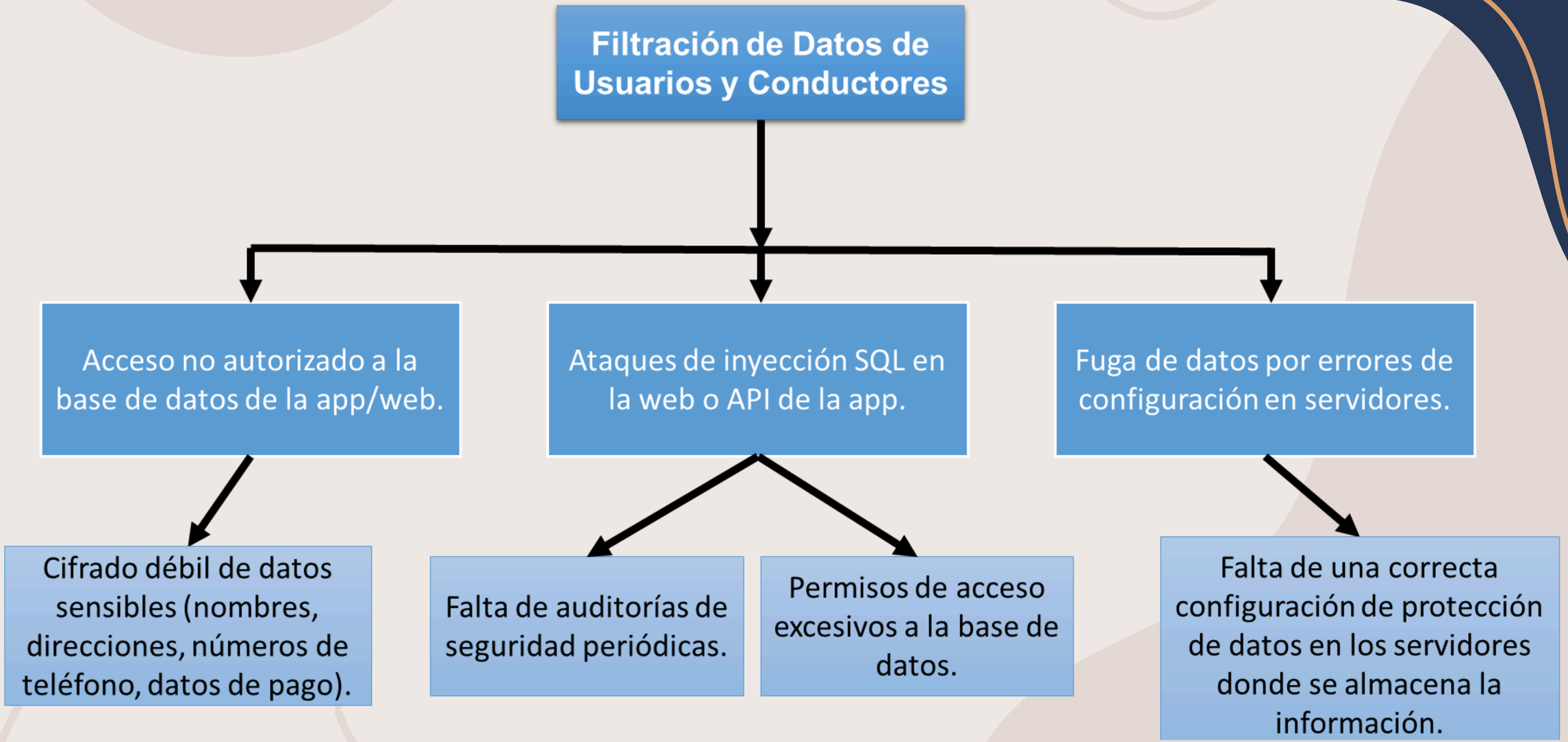
ACTIVOS

ID	Nombre	Descripción	Niveles de confianza
1	Datos de usuarios	Incluye credenciales, información personal y preferencias.	(4) Administrador (2) Usuario registrado
2	Historial de viajes	Registro de viajes realizados.	(2) Usuario registrado (4) Administrador
3	Datos de ubicación	Ubicaciones en tiempo real de taxis y clientes.	(2) Usuario registrado (3) Usuario registrado (taxista) (4) Administrador
4	Transacciones	Registros de pagos y métodos de pago asociados.	(2) Usuario registrado (4) Administrador
5	Reportes de incidencias	Reportes de objetos perdidos o problemas con el servicio	(4) Administrador
6	Documentos de taxistas	Información de registro y verificación de conductores.	(4) Administrador (3) Usuario registrado (Taxista)
7	Calificaciones y comentarios	Evaluaciones de clientes y taxistas.	(2) Usuario registrado (4) Administrador

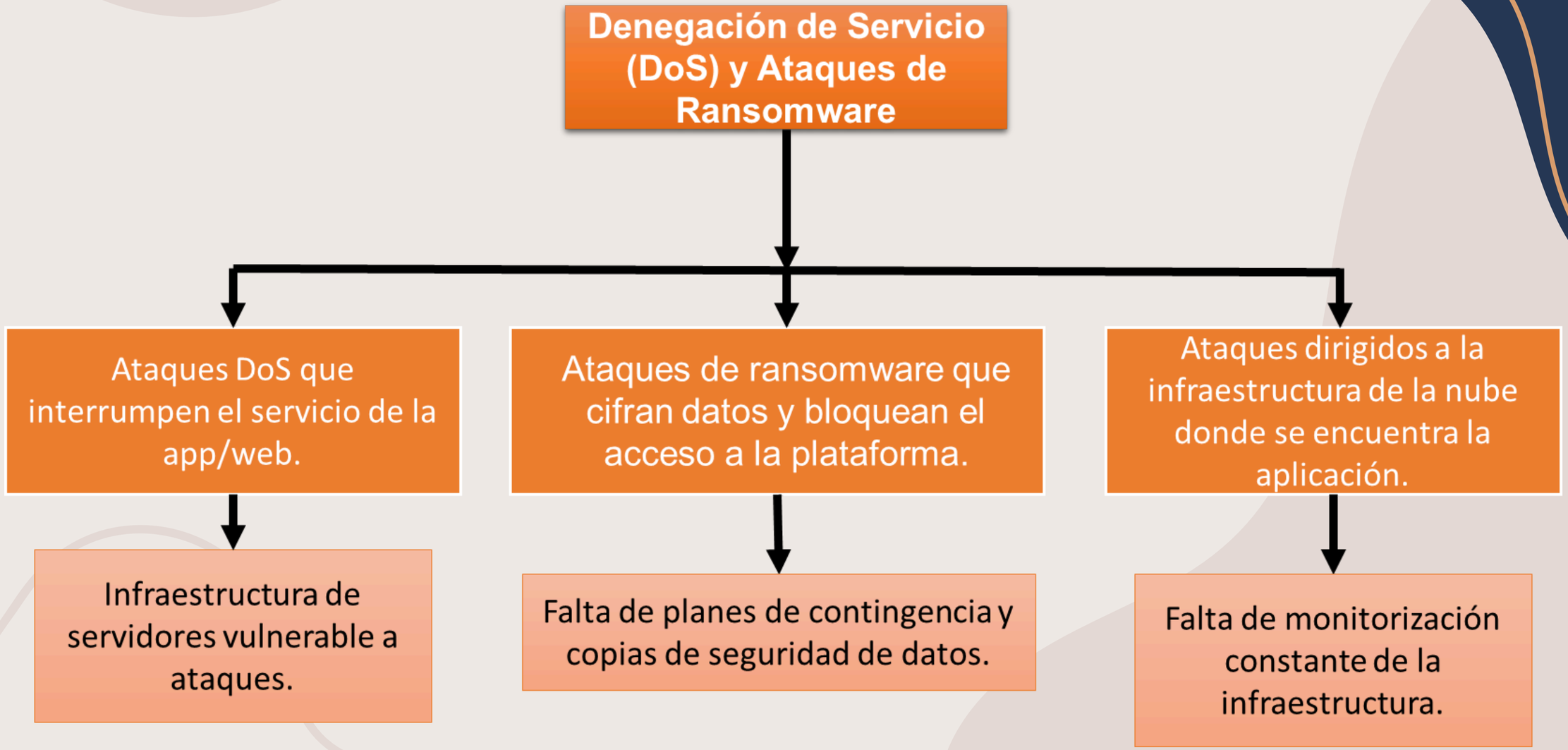
DESGLOSE DE PERMISOS

ID	Nombre	Descripción
1	Usuario anónimo	Usuario que no ha iniciado sesión, solo puede ver información pública
2	Usuario registrado	Cliente autenticado que puede usar funcionalidades principales.
3	Usuario registrado (Taxista)	Taxista autenticado con permisos adicionales para gestionar viajes y disponibilidad.
4	Administrador	Usuario con acceso a la gestión y monitoreo de la plataforma.

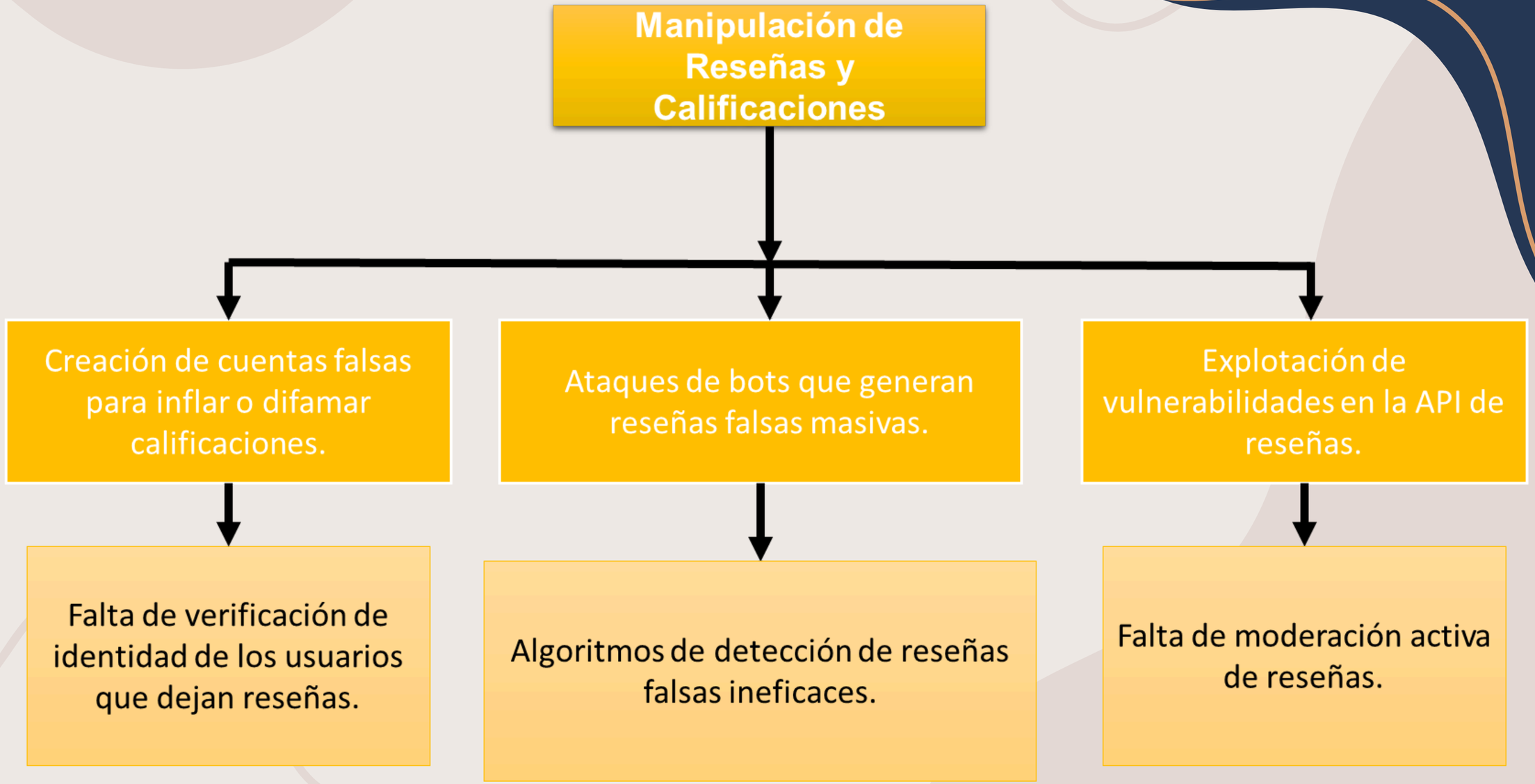
ÁRBOL DE AMENAZAS



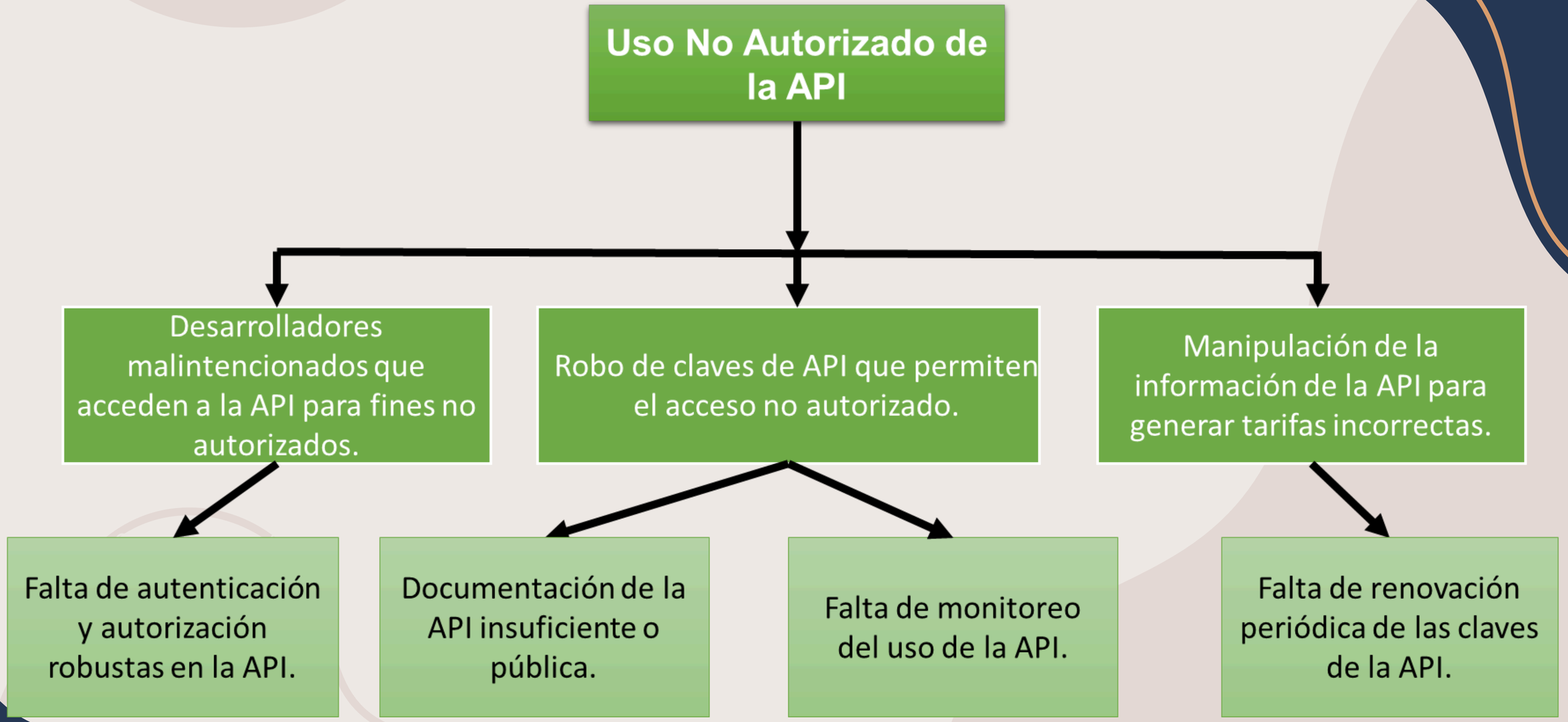
ÁRBOL DE AMENAZAS



ÁRBOL DE AMENAZAS



ÁRBOL DE AMENAZAS



STRIDE

S – SPOOFING – SUPLANTACIÓN DE IDENTIDAD

Amenaza:	Suplantación de identidad (Spoofing)
Propiedad afectada	Autenticación
Definición:	Un atacante suplanta la identidad de un usuario o conductor para acceder a la aplicación.
Ejemplo de la app:	Un atacante usa credenciales robadas para acceder a la cuenta de un conductor y aceptar viajes en su nombre.

T - TAMPERING - MANIPULACIÓN

Amenaza:	Manipulación de datos (Tampering)
Propiedad afectada:	Integridad
Definición:	Modificación no autorizada de datos dentro de la aplicación.
Ejemplo de la app:	Un usuario malintencionado modifica la base de datos para alterar calificaciones y reseñas de conductores o pasajeros.

R – REPUDIATION – REPUDIO

Amenaza:	Negación de acciones realizadas (Repudiation)
Propiedad afectada:	No repudio
Definición:	Un usuario niega haber realizado una acción dentro de la aplicación.
Ejemplo de la app:	Un pasajero niega haber realizado un pago o un conductor niega haber aceptado un viaje.

I – INFORMATION DISCLOSURE – DIVULGACIÓN DE INFORMACIÓN

Amenaza:	Filtración de datos (Information Disclosure)
Propiedad afectada:	Confidencialidad
Definición	Exposición de información a personas no autorizadas.
Ejemplo de la app:	Una vulnerabilidad permite que terceros accedan a datos personales de conductores y pasajeros, como direcciones o números de teléfono.

D – DENIAL OF SERVICE – NEGACIÓN DE SERVICIO

Amenaza:	Ataque de denegación de servicio (DoS9
Propiedad afectada:	Disponibilidad
Definición	Degradación o interrupción del servicio.
Ejemplo de la app:	Un atacante envía múltiples solicitudes falsas para sobrecargar los servidores y hacer que la aplicación deje de funcionar.

E - ELEVATION OF PRIVILEGES - ELEVACIÓN DE PRIVILEGIOS

Amenaza:	Uso no autorizado de la API (Elevation of Privileges)
Propiedad afectada:	Autorización
Definición:	Un usuario obtiene permisos sin autorización.
Ejemplo de la app:	Un pasajero logra modificar parámetros en la API y se otorga permisos de conductor sin validación.