



Tecnológico
de Monterrey

TC2007B.402

Integración de seguridad informática en redes y sistemas de software

Etapa Final - Dif+ App

Luis Fernando De León Silva - A01754574

Carlos Ernesto Soto Alarcón - A01747990

Ernesto Juarez Torres - A01754887

Juan Carlos Carro Cruz - A01748640

20 de Octubre del 2023

Índice

Etapa 1

- Problemática a resolver
- Requerimientos Funcionales
- Requerimientos No Funcionales
- Selección de Hardware y Software
- Alcance de la Aplicación
- Matriz de Riesgos
- Diagrama de Gantt del proyecto

Etapa 2

- Diagrama de Base de Datos
- Diagrama estructural de la página/app web
- Diagrama de clases de Dif+ App
- Diseño de las interfaces de usuario
- Integración de seguridad informática
- Diseño de interfaz web

Etapa 3

- Configuración de la infraestructura de Dif+ App
- Identificación y mitigación de posibles ataques informáticos
- Reuniones con el cliente
- Reuniones con el equipo de desarrollo

Etapa 4

- Planes de prueba
- Casos y datos de prueba
- Resultado de las pruebas
- Informe y cierre de pruebas

Etapa Final

- Capacitación

Aportaciones Individuales

Etapas 1

Problemática a resolver.

En el contexto actual, donde se experimenta una crisis alimentaria global, México no se escapa de esta realidad, mostrando una marcada desigualdad económica en su población. Esta disparidad económica se traduce en una inseguridad alimentaria que afecta alrededor del 25% de la población en el Estado de México. Dada esta situación, la implementación de programas de apoyo social se convierte en una necesidad imperante para suplir las carencias de la población. Los comedores comunitarios surgen como una respuesta a esta necesidad, con el propósito fundamental de "fortalecer el cumplimiento efectivo de los derechos sociales que potencien las capacidades de las personas en situación de pobreza, de la población del Municipio de Atizapán de Zaragoza a través de acciones que inciden positivamente en la alimentación".

Sin embargo, este proyecto de envergadura social no está exento de desafíos internos, especialmente en lo que respecta a la logística, tal como se ha mencionado. Por lo tanto, en esta propuesta, se destaca como el problema primordial a resolver la optimización del proceso de registro de los beneficiarios de los comedores comunitarios. Este refinamiento permitiría mantener datos siempre actualizados, lo que a su vez facilita la toma de decisiones informadas. Actualmente, la falta de un sistema digitalizado de registro ha llevado a dificultades internas, como la incapacidad para contabilizar de manera precisa el número de comidas distribuidas.

En este escenario, en el contexto del DIF de Atizapán de Zaragoza, se presenta una problemática crítica relacionada con la ausencia de un sistema eficiente de registro y control de beneficiarios en los comedores comunitarios. La carencia de este sistema adecuado de registro trae consigo varios desafíos significativos que repercuten directamente en la viabilidad y continuidad del programa.

En primer lugar, la falta de un registro confiable y actualizado complica la justificación para la obtención de los recursos necesarios para mantener en funcionamiento los comedores comunitarios. La carencia de datos precisos sobre la cantidad de beneficiarios, sus características y la frecuencia de consumo dificulta la presentación de informes sólidos y la solicitud de recursos financieros adecuados.

Además, esta problemática afecta la planificación de recursos. La falta de información precisa sobre la cantidad de beneficiarios en cada comedor dificulta la distribución eficaz de recursos, como alimentos y personal. Esto podría resultar en una asignación inapropiada de suministros, comprometiendo la satisfacción de las demandas reales.

La administración de los comedores también se ve perjudicada debido a la ineficiencia causada por la falta de un sistema de registro efectivo. La incapacidad para anticipar las necesidades diarias, controlar el suministro de alimentos y garantizar la atención adecuada a los beneficiarios obstaculiza el funcionamiento fluido y eficaz de los comedores.

De manera similar, la ausencia de un sistema sólido de registro dificulta la evaluación del impacto real del programa en la población atendida. La incapacidad para rastrear la cantidad de beneficiarios y analizar su evolución a lo largo del tiempo dificulta la medición precisa de los resultados y los cambios positivos que el programa puede estar generando en términos de seguridad alimentaria y bienestar.

Frente a esta problemática, resulta crucial la implementación de un sistema de registro centralizado y sistematizado para los beneficiarios de los comedores comunitarios. Esto implica el desarrollo de un sistema digital que permita recopilar y gestionar de manera efectiva los datos de cada beneficiario, incluyendo información demográfica y detalles sobre su consumo. Además, es esencial brindar capacitación al personal encargado de los comedores para garantizar un registro preciso y completo.

La adopción de una solución tecnológica podría acelerar y optimizar el proceso de registro y gestión de datos. La generación regular de informes basados en los datos recopilados ayudaría a respaldar la solicitud de recursos y a demostrar el impacto positivo del programa en la comunidad. En última instancia, el establecimiento de un sistema de registro sólido no solo aborda los desafíos actuales, sino que también allana el camino hacia un programa de comedores comunitarios más efectivo y sostenible.

Requerimientos Funcionales

El sistema (la aplicación) deberá registrar la CURP del usuario, que a su vez, será recolectada por el DIF de Atizapán para medir la afluencia de los comedores comunitarios. A su vez, esto será necesario para poder tomar decisiones en un futuro.

El sistema también deberá desplegar un código QR generado por la misma aplicación que servirá como pieza fundamental para el registro de un usuario al momento del pago.

El sistema deberá servir con los QR que vienen dados en la CURP expedida por el gobierno.

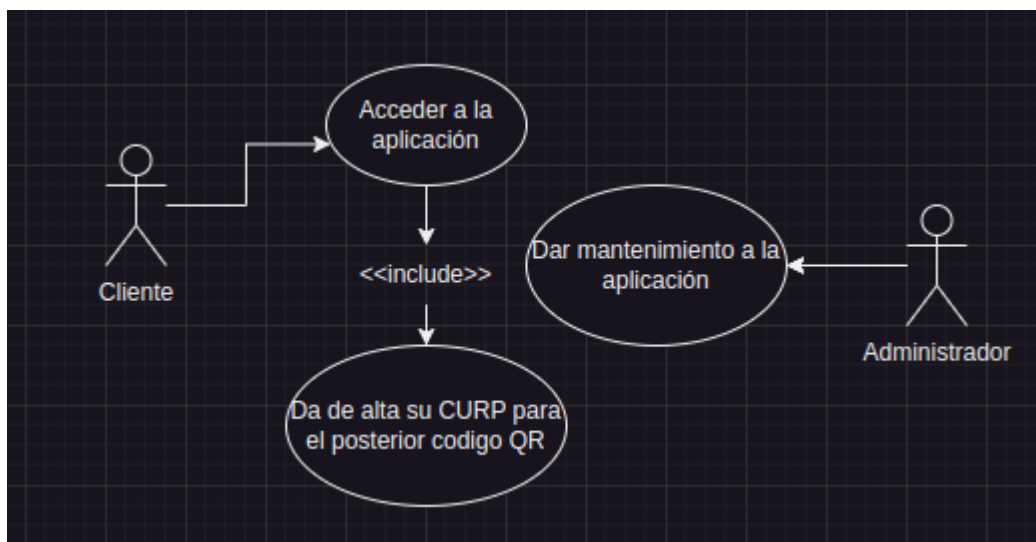


Figura 2.1 Diagrama de Caso de Uso

a) **Caso de Uso:** Registro de un usuario para el comedor.

Precondiciones: Actores: Cliente

Objetivo: Dar de alta el código QR como pase al comedor

Descripción: La aplicación móvil se puede descargar en la tienda desde Google Play, la tienda de aplicaciones de Android. El usuario también puede, si lo desea, acceder a la aplicación desde las tabletas que se encuentran en el mismo comedor. La aplicación contiene solamente un campo de entrada y se le pedirá su CURP o su nombre en dado caso que no recuerde lo anterior. Una vez el usuario registre sus datos, la aplicación mostrará un código QR único conteniendo toda la información del registro para que pueda ser posteriormente escaneada antes de acceder al comedor. A su vez, la aplicación se encargará de enviar los datos correspondientes para fines estadísticos.

Curso de los eventos:

Acción del actor

Respuesta del sistema

1. Abrir la aplicación
2. Da de alta su CURP / Nombre
3. Genera un código QR con el registro.

b) Caso de Uso Detallado: Mantenimiento de la aplicación

Precondiciones: Actores: Administrador

Objetivo: Dar mantenimiento a la aplicación web

Descripción: Con el paso del tiempo, muchas de las dependencias de la aplicación, así como los hipervínculos que se encuentran dentro de la misma. Por esta razón, el administrador del programa tendrá que actualizar estos hipervínculos desde el código fuente de la aplicación, así como las dependencias en formato .kts.

Curso de los eventos:

Acción del actor	Respuesta del sistema
1. Abrir el editor Android Studio (AS)	
2. Sincronizar todas las dependencias	AS hará modificaciones al código fuente

Historia de usuario

COMENSAL

Registro Rápido con CURP y Generación de Código QR

Descripción: Como comensal en el Comedor Comunitario, quiero poder registrar fácilmente mi CURP para acceder a los servicios del comedor y obtener un código QR que me permita obtener mi alimento de manera eficiente.

Criterios de Aceptación:

- La interfaz de registro solicita al comensal ingresar su CURP.
- Tras un registro exitoso, se genera un código QR único y se muestra en la pantalla.
- El código QR es esencial para que el comensal pueda escanearlo y obtener su alimento en el comedor.
- El código QR debe ser fácilmente legible por dispositivos de escaneo.
- Se muestra un mensaje de confirmación o éxito al comensal después de completar el registro.

Dentro de la aplicación del Comedor Comunitario, los usuarios comensales encuentran una manera ágil y eficiente de acceder a los servicios proporcionados. Una vez que ingresan a la

aplicación, son recibidos con la opción de "Registrar con CURP", lo que les brinda una forma rápida de comenzar.

Al seleccionar esta opción, se les presenta un campo de texto donde pueden ingresar su CURP. El sistema valida automáticamente el formato del CURP para asegurarse de que sea correcto. Luego, el sistema verifica en su base de datos si el CURP está asociado a un comensal registrado.

Una vez que se confirma la validez del CURP y su correspondencia con un comensal registrado, el sistema genera al instante un código QR único. Este código QR contiene información específica para identificar al comensal en el sistema del comedor. Los usuarios pueden optar por guardar o descargar el código QR en su dispositivo móvil.

Este proceso de registro y generación de código QR es casi instantáneo, asegurando que los usuarios no tengan que esperar mucho tiempo. Después de completar exitosamente el proceso, el comensal recibe un mensaje claro de confirmación que indica que el registro se ha realizado con éxito y que ahora poseen un código QR válido para acceder a los servicios del comedor.

ADMINISTRADOR

Optimización de la Distribución de Recursos en Comedores Comunitarios

Descripción: Como administrador del Comedor Comunitario, deseo poder utilizar la función de geolocalización para identificar los comedores disponibles en un mapa y optimizar la distribución de recursos, como alimentos y personal, para atender de manera eficiente a los comensales.

Criterios de Aceptación:

- La interfaz de geolocalización debe ser accesible desde la pantalla principal del administrador.
- Al seleccionar la opción de geolocalización, se redirige al administrador a una vista del mapa de Google Maps.
- En el mapa, se muestran marcadores o pins para cada comedor comunitario disponible.
- Al hacer clic en un marcador, se muestra información detallada sobre ese comedor, como su dirección y horarios de operación.
- La información debe ser actualizada y precisa en todo momento para reflejar los cambios en la disponibilidad de comedores.
- La función de geolocalización debe estar integrada con los datos del sistema del comedor para ofrecer una vista en tiempo real de la ubicación y disponibilidad de los comedores.

La Aplicación del Comedor Comunitario está diseñada para simplificar la gestión de recursos y servicios para los administradores. Para lograrlo, se ha implementado una función de geolocalización que permite a los administradores identificar de manera rápida y precisa todos los comedores comunitarios disponibles en un mapa interactivo.

Desde la pantalla principal de la aplicación, los administradores pueden seleccionar la opción de "Geolocalización de Comedores". Al hacerlo, son redirigidos a una vista del mapa de Google Maps, donde se visualizan marcadores o pins que representan cada comedor comunitario.

Al hacer clic en un marcador específico, se despliega información detallada sobre ese comedor en particular. Esto incluye su dirección exacta y los horarios de operación. Esta información es crucial para los administradores, ya que les permite planificar y distribuir eficientemente los recursos, como alimentos y personal, para satisfacer las necesidades de los comensales en cada ubicación.

La funcionalidad de geolocalización se mantiene actualizada y precisa en todo momento, lo que significa que cualquier cambio en la disponibilidad de comedores se refleja de inmediato en el mapa. Esta integración en tiempo real con el sistema del comedor asegura que los administradores cuenten con información confiable y actualizada para tomar decisiones informadas.

Coordinador de Comedor Comunitario

Objetivo: Permitir al Coordinador del Comedor Comunitario registrar y gestionar a las personas que asisten, llevar un inventario de los no perecederos y enviar reportes al DIF central.

Historia:

Como Coordinador del Comedor Comunitario, quiero poder utilizar un sistema digital para registrar a las personas que asisten, distinguir entre ayudantes y comensales, y gestionar el inventario de no perecederos. Además, necesito enviar reportes al DIF central para que puedan distribuir recursos de manera efectiva.

Criterios de Aceptación:

- Puedo iniciar sesión en el sistema con credenciales válidas.
- Al escanear el QR de una persona, se debe cargar su información automáticamente si ya está registrada en el sistema.
- Puedo registrar a una persona nueva proporcionando su nombre, edad y dirección.
- Puedo asignar a una persona como "Ayudante" o "Comensal" durante el registro.
- Puedo ver y editar la lista de personas registradas en el comedor.
- Puedo realizar un seguimiento de la asistencia de cada persona.
- Puedo actualizar la cantidad de no perecederos en el inventario.
- Puedo generar un informe de inventario de no perecederos para enviar al DIF central.

- Puedo generar un informe de asistencia mensual para enviar al DIF central.
- Puedo comunicarme con el DIF central para enviar los informes de manera segura y confiable.

El sistema debe ser intuitivo y fácil de usar para que cualquier miembro del personal del comedor comunitario pueda operarlo.

La información de las personas registradas debe mantenerse confidencial y segura.

Los informes deben proporcionar una visión clara y concisa de la asistencia y el inventario.

Se deben implementar medidas de seguridad, como encriptación y autenticación, para proteger la información y los informes enviados al DIF central.

Requerimientos No Funcionales

El sistema (aplicación) deberá ejecutarse sin problemas en dispositivos móviles Android con la versión 7.0 Nougat o superior para garantizar un buen funcionamiento y rendimiento a la hora de realizar el registro. Si el dispositivo cuenta con Android 6.1 o inferior, el rendimiento no será el óptimo y disminuirá dependiendo la versión del mismo.

El sistema (aplicación) podrá tener soporte para más de 1000 usuarios conectados al mismo tiempo sin ningún problema. Es necesario comentar que todos los usuarios conectados podrán enviar datos sin algún percance.

Selección de hardware y software

La aplicación será desarrollada en Android Studio, un ambiente de desarrollo (IDE) basado IntelliJ IDEA para la plataforma Android. Cuenta con herramientas para desarrollar, compilar y probar software antes de ser lanzado al mercado. A su vez, cuenta con modificaciones específicas para ser compatible con dispositivos Android.

El sistema contará con una base de datos hecha en MariaDB, un DBMS de código abierto similar a MySQL con características más avanzadas y extensiones. Soporta una gran variedad de lenguajes y también emplea una versión estándar de SQL. MariaDB fue desarrollado para reemplazar y mejorar los defectos que MySQL presentaba tanto en el desarrollo de bases de datos como en el rendimiento mismo. El equipo de Dif+ App considera que MariaDB es el DBMS indicado para este proyecto en concreto.

Nuestro equipo de hardware emplea AWS (Amazon Web Services), nos proporciona un servicio de alojamiento de bases de datos dentro de un servidor basado en una nube; en concreto RDS (Relational Database Services), lo cual es compatible con entornos de desarrollo virtuales con VMware. RDS soporta PostgreSQL, MySQL, MariaDB, SQL Server y servicios de BD de Oracle. A su vez, el mismo sistema web está montado en una instancia de EC2 para conexiones remotas seguras empleando una llave SSH.

Alcance de la Aplicación

La Aplicación del Comedor Comunitario está diseñada para ofrecer una experiencia integral tanto para comensales como para administradores del comedor. Su objetivo principal es facilitar la gestión y optimización de los recursos y servicios del comedor mediante una serie de módulos específicos.

1. Registro Mediante CURP:

- Permite a los comensales introducir su CURP para acceder a los servicios del comedor.
- Generación y visualización de un código QR tras el registro exitoso del comensal, esencial para obtener su alimento.

2. Geolocalización de Comedores:

- Proporciona un enlace que redirecciona al mapa de Google Maps.
- Muestra todos los comedores disponibles, permitiendo al comensal identificar el más cercano.

3. Acceso Administrativo:

- Autenticación de usuarios administrativos a través de una clave.
- Pantalla de inicio de sesión administrativa que solicita: nombre, correo, contraseña y No. de comedor.

4. Interfaz Principal Administrativa:

- Visualización de datos del administrador: fotografía de perfil, nombre y dirección de correo electrónico.
- Cuatro opciones principales: "Tablero", "Personal", "Recaudaciones" e "Inventario". A su vez, existe un "login" de registro y un apartado para cerrar la sesión de administrador.

5. Módulo de Tablero

6. Módulo de Personal

7. Módulo de Recaudaciones

8. Módulo de Inventario

9. Cerrar Sesión:

- Permite al administrador salir de la sesión y regresar a la pantalla principal.

Con estos módulos y características, la aplicación busca ofrecer una experiencia integral tanto para comensales como para administradores, facilitando la gestión y optimización de los recursos y servicios del comedor comunitario.

Matriz de Riesgos

Riesgo	Probabilidad de Ocurrencia	Impacto Potencial	Estrategia de Mitigación
Fallo en la autenticación de usuarios.	Alta	Alto	Implementar sistemas robustos de autenticación y encriptación.
Pérdida de datos de los comensales.	Media	Alto	Implementar copias de seguridad y protocolos de recuperación.
Pérdida de datos de los comensales.	Baja	Medio	Implementar copias de seguridad y protocolos de recuperación.
Sobrecarga de la plataforma por alto tráfico.	Media	Alto	Optimizar el rendimiento y escalabilidad del servidor.
Códigos QR no reconocidos por los lectores.	Baja	Medio	Implementar estándares universales de códigos QR.
Errores en la geolocalización de los comedores.	Media	Medio	Utilizar proveedores de mapas confiables y realizar pruebas.
Brecha de seguridad y acceso no autorizado.	Baja	Muy Alto	Utilizar proveedores de mapas confiables.
Brecha de seguridad y acceso no autorizado.	Media	Bajo	Utilizar proveedores de mapas confiables y realizar pruebas.
Brecha de seguridad y acceso no autorizado.	Baja	Bajo	Realizar pruebas exhaustivas de la interfaz de usuario.
Cambios en las	Baja	Alto	Realizar pruebas

regulaciones de protección de datos.			exhaustivas de la interfaz de usuario.
Limitaciones de recursos en cuanto al equipo/tabletas que requieren los comedores	Media	Alto	Utilizar los equipos celulares de los que disponga el personal del comedor para el uso de nuestro software.
Falta de capacitación del personal para el uso de nuevas tecnologías	Media	Medio	Elaborar un software que sea lo más amigable, intuitivo y sencillo posible con cualquier usuario, esto desde el diseño del mismo.
Falta de mantenimiento del software en general	Media	Alto	Implementar sistemas robustos y eficientes además de contar con personal capacitado que constantemente pueda dar mantenimiento a largo plazo.
Inadecuada colaboración entre el personal en cuanto a comunicación efectiva y el uso del software	Baja	Medio	Elaborar nuestro software de manera que sea lo suficientemente explicativo e intuitivo para el personal además de brindar constantemente apoyo técnico y capacitación para poder minimizar riesgos de mala comunicación.

Diagrama de Gantt del proyecto

El proyecto se va a dividir en 7 etapas: Requerimientos, Diseño, Código, Pruebas, Despliegue, Documentación y Mantenimiento. Todos los miembros del equipo tendrán responsabilidades en cada una de las etapas y subetapas.

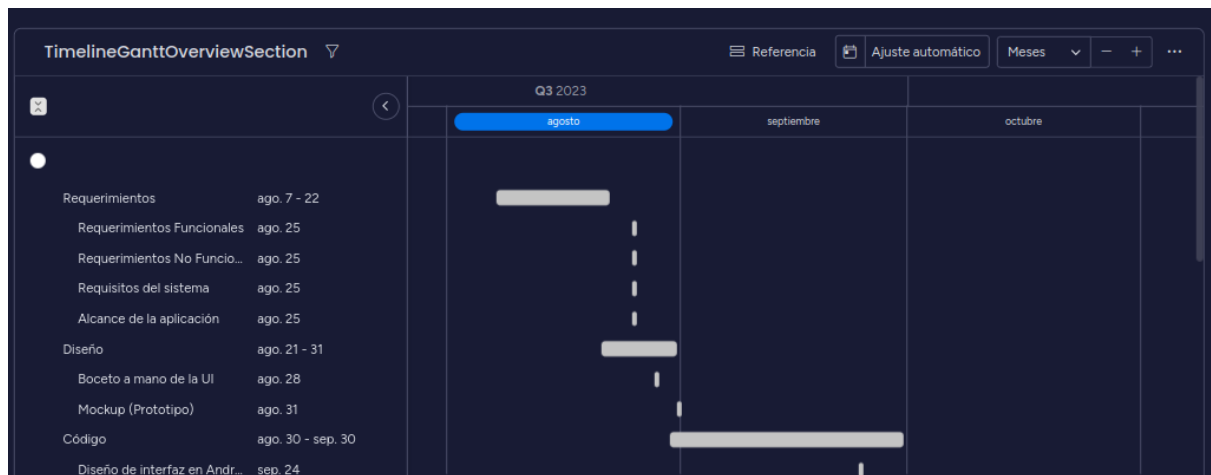


Figura 2.1 Etapas entre Ago 7 y Sep 24

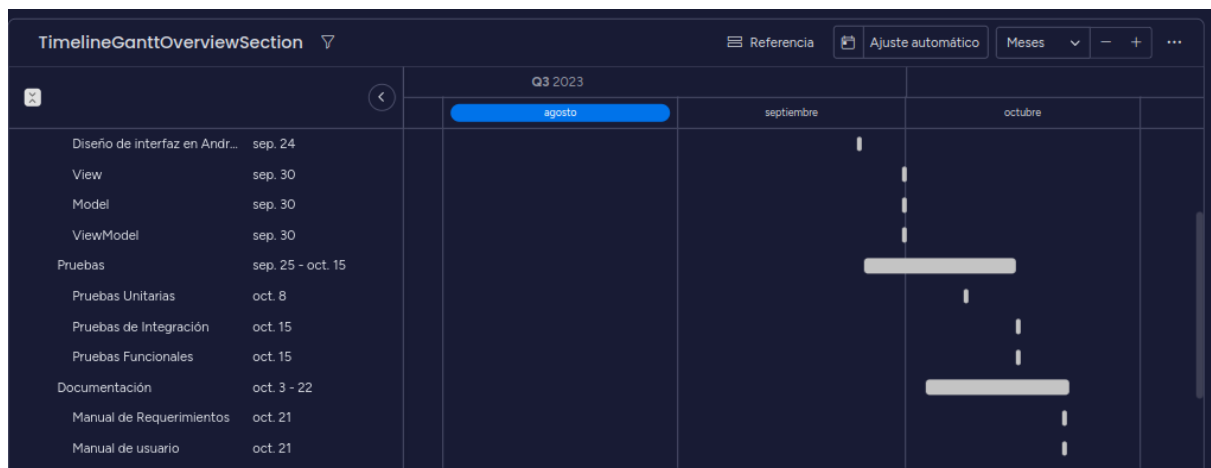


Figura 2.2 Etapas entre Sep 24 y Oct 21

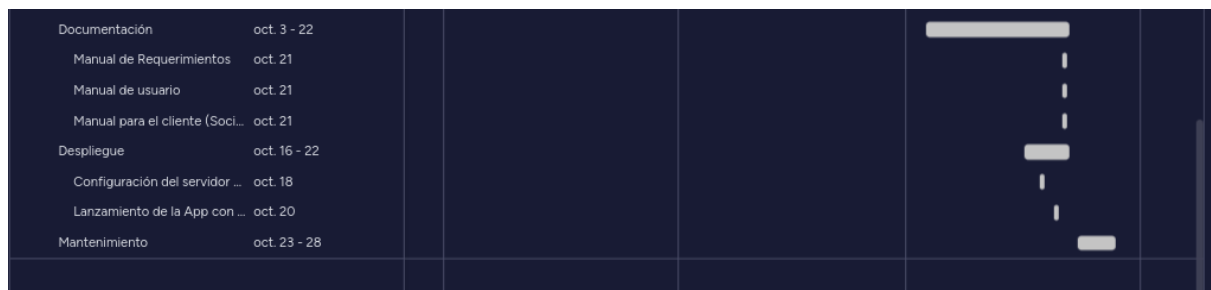


Figura 2.3 Etapas entre Oct 3 y Oct 28

Cada una de las etapas tendrán subtareas específicas que conformarán todo el proyecto. El reporte de estatus, así como las fechas límite para cada actividad. Conforme el proyecto vaya

avanzando, el diagrama se irá actualizando respecto a las actividades que vayan siendo completadas.

Prototipo

Dif+ App comensal

https://www.canva.com/design/DAFt5r5V8hs/eZwC9oXrUVgcfQiwH2mXbg/view?utm_content=DAFt5r5V8hs&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink

Dif+ App empleado

https://www.canva.com/design/DAFt5QULJUw/s3V5ttVtkMWUEgh4ToLudQ/view?utm_content=DAFt5QULJUw&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink

Página web

https://www.canva.com/design/DAFyDAMI7gQ/yA3wqacOvnO22Clrl_hw5g/view?utm_content=DAFyDAMI7gQ&utm_campaign=designshare&utm_medium=link&utm_source=editor

Etapas 2

Diagrama de Base de Datos

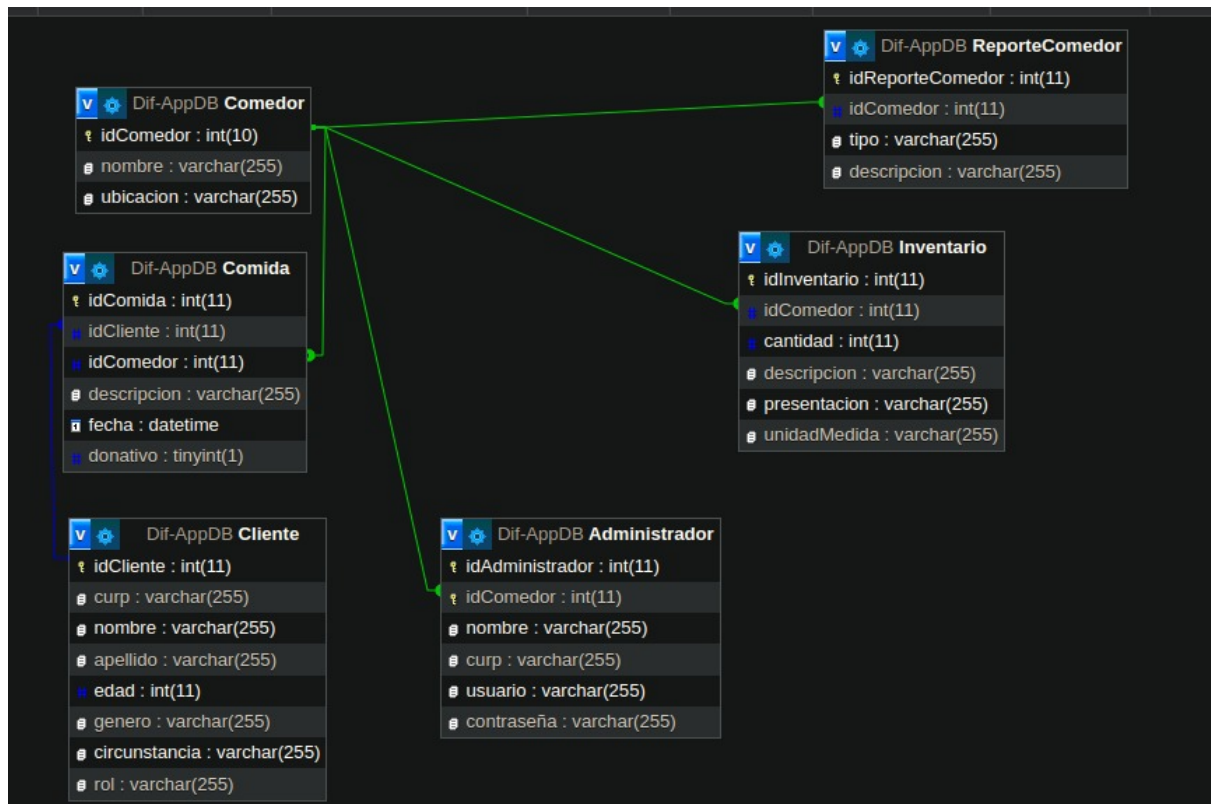


Figura 3.1 Diagrama de la base de datos

Arquitectura de Dif+ App

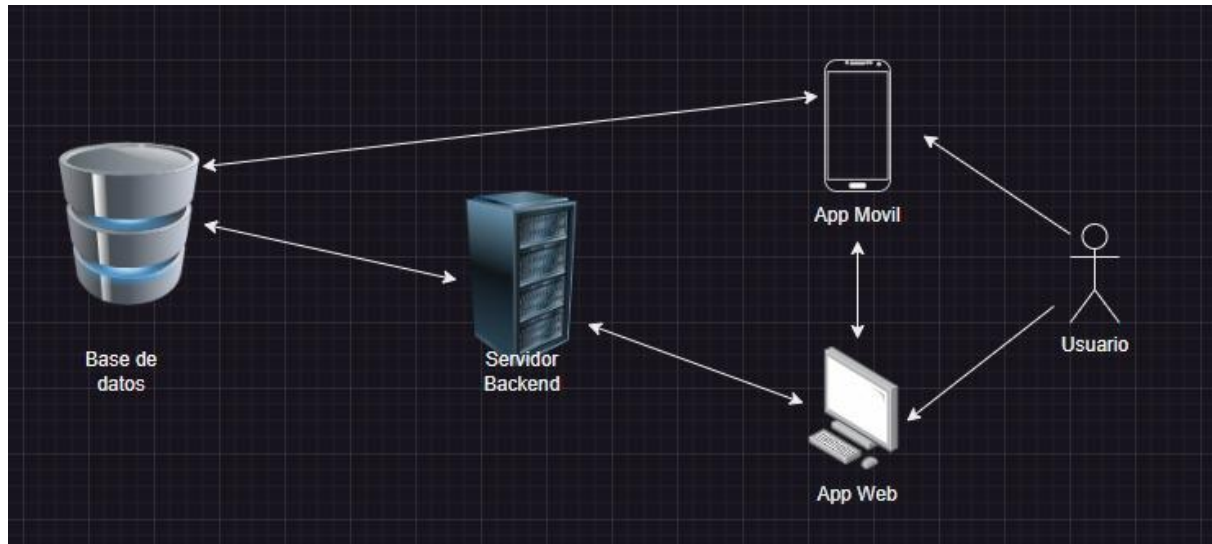


Figura 3.2 Arquitectura del sistema de Dif+ App

Diagrama estructural de la página/app web

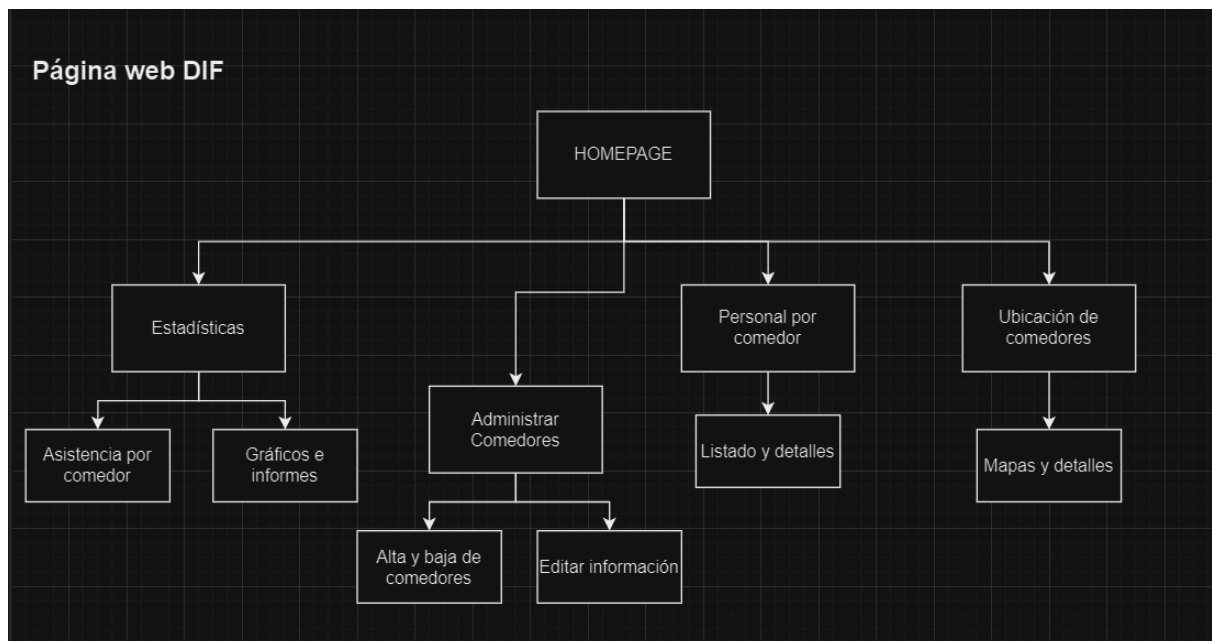


Figura 3.3 Diagrama estructural de la página web

Arquitectura de Capas para el Sistema de Registro de Pagos y Estadísticas:

Capa de Presentación (Interfaz de Usuario):

- Aplicación de Cliente (Genera QR) (Android Studio con Kotlin):
- Esta app permite a los clientes generar códigos QR. La interfaz de usuario permite ingresar la información necesaria y genera el código QR correspondiente.
- Utiliza lenguaje Kotlin y Android Studio para el desarrollo de la interfaz y la lógica de generación de QR.

Aplicación de Comedor (Registra QR con Pago) (HTML, CSS, JavaScript):

- En esta app, los comedores escanean el código QR generado por la app del cliente y registran la transacción junto con la información de pago.
- La interfaz de usuario está construida con HTML para la estructura, CSS para el diseño y JavaScript para la interactividad.

Capa de Lógica de Negocio (o Capa de Servicios):

- Backend (Flask en Python):
- Esta capa se encarga de la lógica de negocio de ambas aplicaciones. Maneja la autenticación, validación de datos, procesamiento de transacciones y comunicación con la base de datos.
- Flask (Python) se utiliza para la construcción de la lógica del servidor.

Capa de Acceso a Datos (SQL para la Base de Datos):

Base de Datos (SQL):

Aquí se almacenan los detalles de las transacciones, los códigos QR generados y otra información relevante. Se deben tener tablas para clientes, transacciones, comedores, etc.

Interconexión entre las Capas:

La app de cliente y la app de comedor se comunican con el backend (Flask) a través de solicitudes HTTP. El backend procesa estas solicitudes, valida los datos y realiza operaciones en la base de datos según sea necesario.

Página Web de Estadísticas (HTML, CSS, JavaScript):

Esta página web se encarga de mostrar las estadísticas y reportes basados en la información almacenada en la base de datos. Utiliza tecnologías web estándar como HTML para la estructura, CSS para el diseño y JavaScript para la interactividad.

Diagrama de Clases de Dif+ App

- La clase Comedor tendrá relación uno-a-muchos tanto con la clase Empleado como con Reporte Comedor, un comedor podrá tener muchos empleados y realizar varios reportes al mismo tiempo
- La clase Cliente tendrá una relación uno-a-muchos con la clase ReporteCliente, ya que un cliente podrá realizar muchos reportes
- La clase Comedor tendrá una relación uno-a-uno con la clase Administrador, ya que solo debe haber un administrador por comedor.

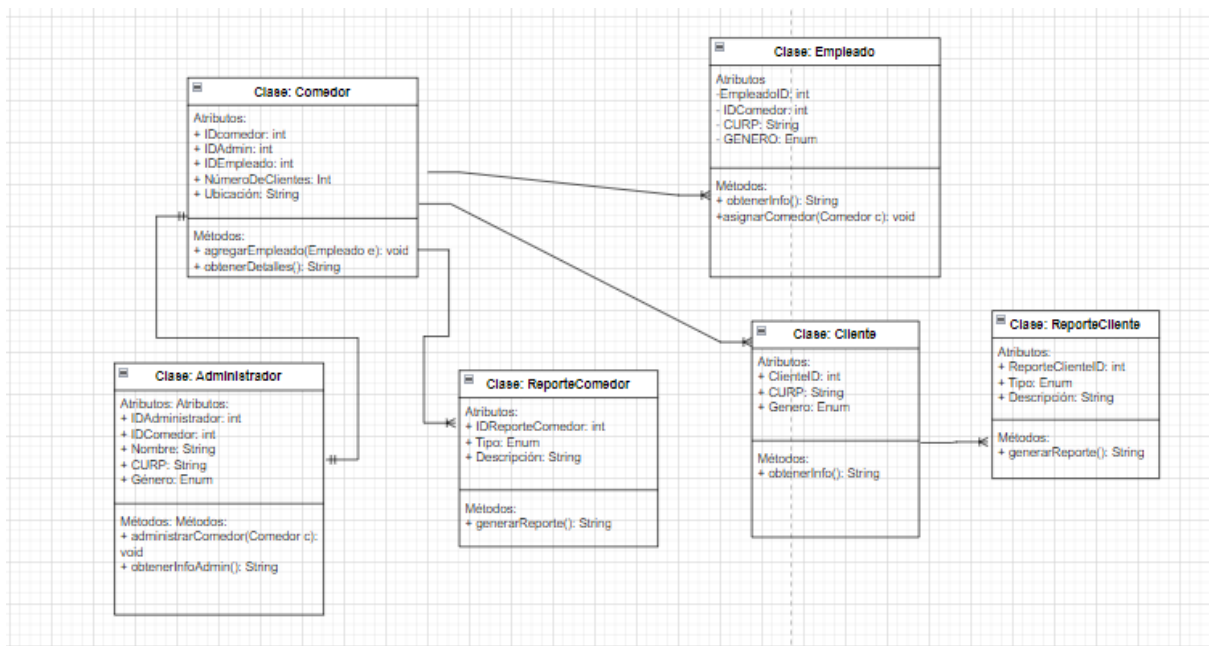


Figura 4.1 Diagrama de clases

Diseño de las interfaces de usuario

1. Diseño de la interfaz para la aplicación móvil para el cliente

8:36

BIENVENIDO



Ingresa tu CURP

Consulta tu CURP en <https://www.gob.mx/curp/>


No tengo CURP

☐ Acepto los Términos y condiciones

Inicia Sesión

Cerrar Sesión

No Cuentas Con CURP



Nombre

Apellido Paterno

Apellido Materno

Sexo

Fecha de Nacimiento

☐ Acepto los términos y condiciones

Registro

Cerrar Sesión

Términos y condiciones

PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES OBJETIVO GENERAL. Implementar los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales del Sistema Nacional para el Desarrollo Integral de la Familia, conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos de Protección de Datos Personales para el Sector Público. Previo a recabar datos personales, se debe mostrar el aviso de privacidad integral y/o simplificado, según sea el caso; el aviso de privacidad debe encontrarse en un lugar visible. 3. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben. 4. Las áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de atribuciones y funciones. 5. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones otorgadas a las áreas del Sistema Nacional DIF. 6. Es obligación de todas las personas servidoras públicas del Sistema que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros. 7. Cuando se recaben datos personales de menores de edad se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre éstos. 8. Las áreas deberán identificar todos los avisos de privacidad que se requieren, según los tratamientos que

Derechos y obligaciones de las personas que asisten a los Comedores Comunitarios

4.5.1 Derechos


- Recibir un trato digno, respetuoso, oportuno, y sin discriminación;
- Acceder a la información necesaria sobre el Programa;
- Proteger sus datos personales de acuerdo a la normatividad aplicable;
- Recibir una ración de comida al día de alimentos preparados en el Comedor, hasta 5 días a la semana;
- Presentar ante la Comisión de Alimentación del Comité Comunitario de su localidad, su solicitud de inclusión al Programa;
- Participar en las actividades asociadas al Programa;

4.5.2 Obligaciones

- Cubrir la cuota establecida por el Comité Comunitario, con recursos económicos, autorizado por el Comité;
- Acatar las medidas higiénicas y sanitarias establecidas en el Comedor;
- Notificar por cualquier medio a la Comisión de Alimentación del Comité Comunitario, en caso de no poder asistir al Comedor, por enfermedad o alguna causa excepcional. Faltar más de 5 días consecutivos sin notificar a la Comisión de Alimentación es causal de suspensión automática del Listado de personas que asisten a los Comedores; podrá solicitar su reingreso de conformidad a lo establecido en el numeral 4.5.1, inciso e);
- Asistir de manera periódica al Comedor, cuando menos 15 días al mes, registrando su asistencia en el Formato respectivo;
- Validar su asistencia mensual mediante firma o huella digital;
- Mantener una actitud de respeto hacia las demás personas que asisten a los Comedores y hacia las personas integrantes de la Comisión de Alimentación;

a) Cumplir con lo dispuesto en el presente instrumento.

MENU Dif+ App



QR


Mapa

Encuesta


Salir

Derechos y Obligaciones

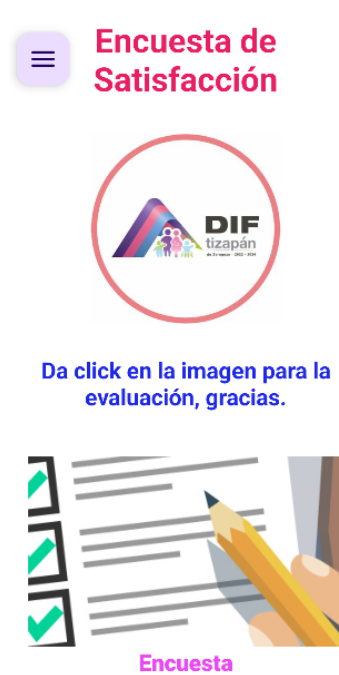
Mapa Comedores



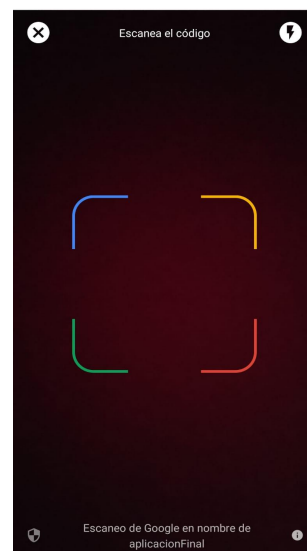
Para encontrar el comedor más cercano, haz clic en la imagen de abajo y localiza tu comedor.




Abrir mapa



2. Diseño de la interfaz para la aplicación móvil para el administrador






EL QR ESCANEADO NO ES VÁLIDO

Escanear de nuevo

SE HA REGISTRADO EL COMENSAL



Número: 15
 Apellido Paterno: CARRO
 Apellido Materno: CRUZ
 CURP: CACJ030610HMCRRNA9
 Nombre Completo: JUAN CARLOS
 Sexo: HOMBRE
 Fecha de Nacimiento: 10/06/2003
 Estado: MEXICO


DONACIÓN: ☒

CONDICIÓN: Ninguna

ESCANEAR COMENSAL

MENU PRINCIPAL

SE HA REGISTRADO EL AYUDANTE




Número: 15
 Apellido Paterno: CARRO
 Apellido Materno: CRUZ
 CURP: CACJ030610HMCRRNA9
 Nombre Completo: JUAN CARLOS
 Sexo: HOMBRE
 Fecha de Nacimiento: 10/06/2003
 Estado: MEXICO

ESCANEAR AYUDANTE

MENU PRINCIPAL

LEVANTAR UN REPORTE



SITUACIÓN: Seleccionar

DESCRIPCIÓN:

Escribe una breve descripción de la situación

CIERRE TEMPORAL: ☒


ENVIAR

MENU PRINCIPAL

PRESENTACIÓN	CANTIDAD
20 LT	
1 KG	
140 GR.	
50 KG.	
400 GR	
400 GR	
2.8 GR	
1 KG	
220 GR	
OR 1.89 LT	
3.5 KG	
400 GR	

3. Diseño de la interfaz para la aplicación web para el administrador

Bienvenido de vuelta!
a Dif+ App



Usuario:

Contraseña:

Iniciar Sesión

Solamente para nuevos administradores: [Regístrate aquí](#)

Bienvenido



Comedor:

Comedor A ▼

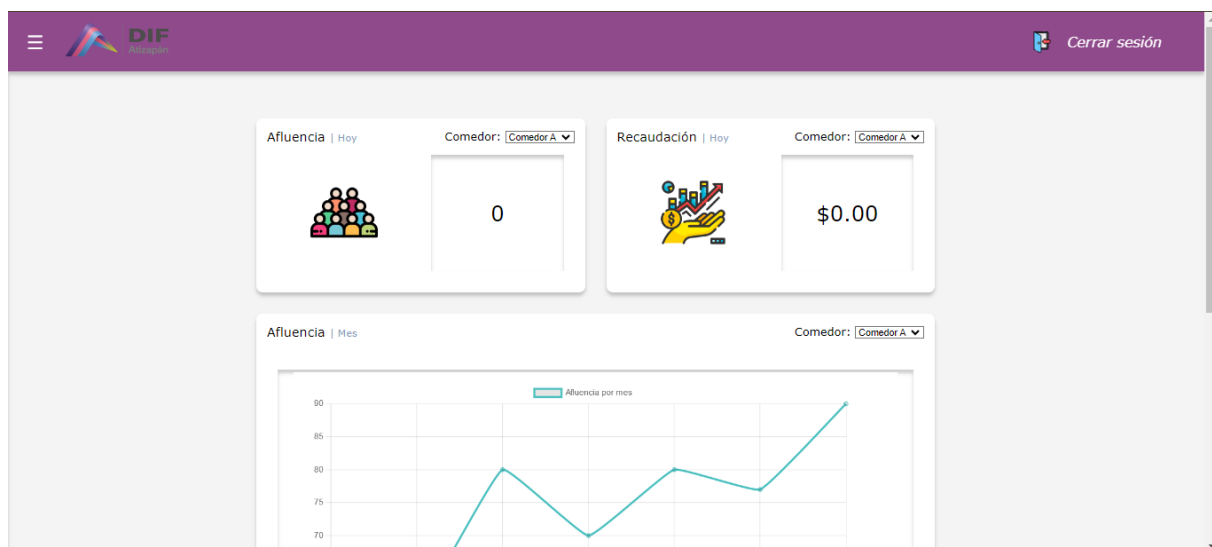
Nombre:


CURP:

Usuario:

Contraseña:

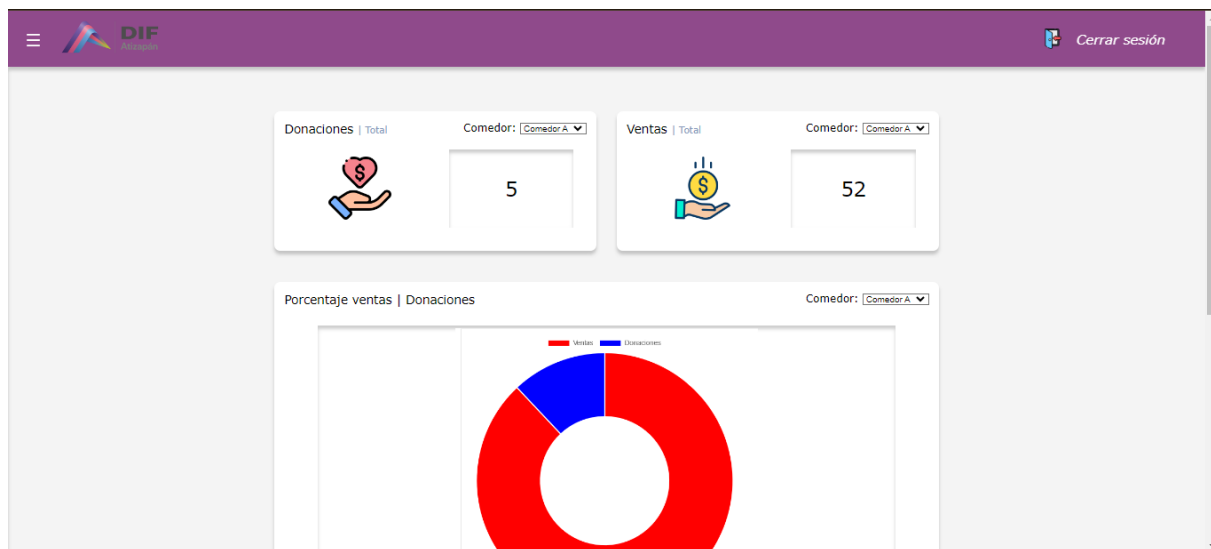
Iniciar Sesión





Cerrar sesión

Administradores | Por comedor
Comedor: Comedor B

Juan Perez	CURPEjemplo
------------	-------------




Cerrar sesión

Inventario | Por comedor
Comedor: Comedor A

Cantidad	Descripción	Presentación	Unidad de Medida
10	Sopa	3 oz	1 PIEZA
20	Agua	500 ml	3 PIEZAS
100	Artículo A	3 oz	PIEZA
150	Artículo D	3 oz	PIEZA
180	Artículo G	3 oz	PIEZA

Integración de seguridad informática

Dif+ App presentará un enfoque totalmente basado en una autenticación de rol ya que todo el sistema no solo cuenta con 1 sino 3 aplicaciones; 2 aplicaciones móvil (Cliente y Administrador) y 1 aplicación web (Administrador/DIF).

La autenticación de rol se basa en lo siguiente:

- Las medidas contra ataques de fuerza bruta y ataques de diccionario están activas, así como bloqueo de cuenta en dado caso de varios intentos fallidos de acceso
- Los administradores contarán con diferentes roles dependiendo de su puesto laboral. Esto quiere decir que tendrán distintos privilegios para realizar determinadas tareas y acciones dentro de la app. También, los administradores con un rol superior podrán tener control total sobre el sistema y así previniendo alguna acción maliciosa.
- El sistema cuenta con una política de contraseñas seguras. Por esto, todas las contraseñas son de 12 caracteres generadas automáticamente. Cada 2 meses, todas las contraseñas se actualizarán automáticamente. De igual manera, cada administrador contará con un nombre de usuario único que le permitirá tener acceso a su cuenta.
- Es importante notar que tanto el usuario como la contraseña serán administrados de manera manual. Es decir, el sistema no se encargará de proporcionar la autenticación y son los propios administradores superiores quienes se van a encargar de esta tarea. Esto se realiza con fines de seguridad al evitar cualquier probabilidad de un ataque que involucra un tercero en el acto, más conocido como un ataque de intermediario (MitM)
- También es importante denotar que los administradores superiores estarán capacitados para mantener e implementar nuevas medidas de seguridad

Es necesario comentar que las 2 aplicaciones móviles tendrán las mismas medidas de seguridad. Sin embargo, es necesario mencionar que la aplicación móvil para administradores tendrá varias medidas más debido a los permisos que se otorgan entre los administradores. Por lo tanto, podemos contar con lo siguiente:

- La seguridad de los datos personales será más que un hecho al incluir bibliotecas robustas para gestionar el ingreso de los usuarios
- Por otra parte, la aplicación móvil para administradores incluirá un segundo factor de autenticación (2FA) además del nombre de usuario y contraseña para añadir más seguridad.
- El código QR será únicamente para validar el registro del cliente. En él, contendrá únicamente la Clave Única de Registro de Población (CURP) y un estatus. La aplicación no permitirá al usuario guardar el código en la galería personal y los demás usuarios no podrán acceder al dicho código generado.
- La aplicación tendrá permisos para abrir aplicaciones tanto de terceros como nativas de Google. Por lo tanto, la aplicación deberá solicitar permiso para abrir la cámara con

el objetivo exclusivo de escanear el código QR. Dicha implementación será en la aplicación de administradores.

- En la aplicación se garantiza que todos los datos personales tanto de los clientes como de los administradores puedan estar protegidos hasta llegar a la base de datos. Por esta razón, ambas aplicaciones cuentan con SSL/TLS, así como una protección en contra de las inyecciones SQL
- La aplicación realiza auditorías para registrar cualquier tipo de acción por parte de los usuarios. Se registra cada actividad realizada con el fin de verificar la autenticidad de los usuarios y prevenir un ataque desde dentro.
- También, la aplicación contará con un cumplimiento normativo, denominado como Reglamento General de Protección de Datos (GDPR)
- Constantemente, la aplicación tendrá pruebas de seguridad constantes para encontrar y reparar alguna vulnerabilidad que permita a los usuarios ilegítimos obtener privilegios. Si existe la posibilidad, se puede aplicar dicha vulnerabilidad a The MITRE Corporation para obtener un número CVE-ID e identificar la vulnerabilidad. Esto significa que la aplicación tendrá actualizaciones de software constantes.
- Así mismo, existirá un control de anomalías UI/UX. Los administradores se encargan de enviar un reporte a los administradores superiores sobre el defecto para poder ser corregido de manera inmediata

Por otra parte, la aplicación web también contará con varias medidas de seguridad. Algunas de ellas son las siguientes:

- La aplicación web cuenta con una administración de usuario segura, empleando tokens de sesión con un tiempo de expiración
- Por otra parte, el acceso a la página web con los privilegios de administrador incluirá un segundo factor de autenticación (2FA) para añadir más seguridad.
- La aplicación cuenta con cifrado SSL/TLS para la protección de los datos, así como un protocolo seguro HTTPS (Hypertext Transfer Protocol Secure). Es decir, los datos de una petición serán enviados con un encriptado.
- La aplicación lleva un registro de auditoría. Al igual que en ambas aplicaciones móviles, se revisan y registran todas las actividades realizadas por los administradores.
- Se maneja de manera automática un control de errores de la arquitectura de la aplicación web para evitar brechas que puedan causar una divulgación de datos sensibles para terceros
- Los administradores de la aplicación web tienen un plan de respuesta a incidentes que detalla cómo abortar un problema o un incidente de seguridad
- Por otra parte, los administradores también realizan respaldos de manera diaria, por lo que si en dado caso, la aplicación web es propensa a errores o a un ataque DoS y DDoS, los datos actualizados dentro del último respaldo serán restablecidos de manera inmediata

La Base de Datos de todo el sistema también contendrá medidas de seguridad. Anteriormente, se mencionó que se reforzarán las medidas para mitigar las inyecciones SQL, pero también existirán otras medidas:

- El acceso a la BD está restringido para los administradores inferiores. Los administradores superiores tendrán acceso una vez hayan sido capacitados para su manejo e interacción. Por otra parte, el acceso incluirá un segundo factor de autenticación (2FA) para añadir más seguridad.
- Todos los datos dentro de la BD serán cifrados, tanto como un cifrado de columnas (cifrado específico) y cifrado de mensajes (algoritmos de cifrado simétrico y asimétrico).
- Es necesario comentar que cuando los datos estén en reposo (Es decir, no exista ninguna comunicación entre la BD y las aplicaciones), se emplea un cifrado a nivel de disco. El disco está alojado en la nube sobre una instancia de EC2.
- Se emplearán protocolos seguros para el manejo de la BD a través de la red. Por eso, HTTPS será el protocolo empleado para el tráfico web y SFTP/SSH para la protección y transferencia de ficheros seguros.
- Para el cifrado de ficheros, se está considerando emplear una biblioteca de cifrado como OpenSSL (para ficheros por separado) y BitLocker (para discos enteros)
- Para el cifrado de contraseñas, se emplearán funciones hash, en concreto SHA-1 y SHA-2. El script con SQL se encargará de crear dichas funciones.
- Para el cifrado y gestión de claves, se emplea el servicio de AWS (Amazon Web Services) KMS (AWS Key Management). Dado que tanto la aplicación Web y la BD estarán en la nube, será indispensable contar con otro servicio en la nube para almacenar la gestión de claves y aprovechar al máximo los recursos disponibles.

Por último, sin importar que parte del sistema ocurra un incidente, es importante denotar que dicho incidente es reportado de manera inmediata para mitigar los daños y ejecutar un plan de respuesta a incidentes.

Etapas 3

URL DEL SOFTWARE

Repo Web: <https://github.com/Its-Yayo/Dif-App-Web>

Repo Cocina: <https://github.com/Its-Yayo/Dif-App-Cocina>

Repo Comensales: <https://github.com/Ernesto-Juarez-Torres-A01754887/Dif-App-Cliente>

Configuración de la infraestructura de Dif+ App

Dado que Dif+ App está desarrollando con el objetivo de ser un sistema seguro pero sobre todo escalable y de fácil mantenimiento, fue para nosotros un reto encontrar las herramientas necesarias. Sin embargo, creemos que la infraestructura que hemos establecido será efectiva para satisfacer estas necesidades. A continuación, se describe la configuración de la infraestructura que hemos utilizado:

- Desarrollo en Android Studio utilizando Kotlin:

Para la creación de la aplicación Dif+ App Comensal y Dif+ App Empleado, utilizamos Android Studio, que es el entorno de desarrollo integrado (IDE) preferido para aplicaciones móviles en el sistema operativo Android. El lenguaje de programación principal que elegimos fue Kotlin debido a su seguridad, eficiencia y facilidad de uso. Esta elección nos permitió desarrollar aplicaciones móviles de alta calidad con una menor probabilidad de errores de seguridad.

- Página web desarrollada en Java:

La página web, que actúa como una interfaz adicional para el proyecto Dif+ App, se desarrolló utilizando el lenguaje de programación Java. Java es ampliamente reconocido por su versatilidad y su capacidad para brindar seguridad en las aplicaciones web.

- Base de datos MongoDB:

Para el almacenamiento y gestión de datos en el proyecto, optamos por MongoDB, una base de datos NoSQL. Esta elección nos permite manejar datos no estructurados y semiestructurados de manera eficiente, lo que es esencial para la flexibilidad requerida por un proyecto de esta naturaleza.

- Hash de contraseñas:

La seguridad de las contraseñas de los usuarios es de suma importancia. Implementamos técnicas de hashing de contraseñas para garantizar que las contraseñas almacenadas en la base de datos estén seguras y no sean susceptibles a exposiciones en caso de un fallo de seguridad.

- Contraseñas seguras en la página web y la aplicación de empleados:

En la página web y la aplicación de empleados, aseguramos que se utilicen contraseñas seguras y que se sigan las mejores prácticas de autenticación para proteger los datos personales y garantizar la integridad de las cuentas de los usuarios.

- Escalabilidad y Facilidad de Mantenimiento:

La infraestructura se ha diseñado pensando en la escalabilidad y facilidad de mantenimiento. Esto implica utilizar tecnologías y arquitecturas que permiten agregar recursos y características fácilmente a medida que el sistema crece. Además, hemos implementado

patrones de diseño y buenas prácticas que facilitan el mantenimiento y las actualizaciones futuras.

Identificación y mitigación de posibles ataques informáticos

La seguridad es una consideración esencial en el desarrollo y despliegue de aplicaciones informáticas. Este subtema describe las estrategias y las mejores prácticas para garantizar la seguridad de dos aplicaciones en particular: la "Aplicación del Comensal" y la "Aplicación de Registro de Empleados" junto con la página web. Las medidas que se describen a continuación están diseñadas para identificar y mitigar posibles amenazas y ataques informáticos.

Aplicación del Comensal (App 1)

Validación del CURP (Clave Única de Registro de Población)

- **Objetivo:** Asegurarse de que el CURP se valida de manera adecuada en la clase de Kotlin, verificando el formato y la estructura correctos.
- **Medidas de Seguridad:** Implementar funciones de validación en Kotlin para comprobar el formato del CURP y garantizar que cumple con los requisitos legales.

Seguridad en el Almacenamiento

- **Objetivo:** Almacenar el CURP y otros datos sensibles de manera segura.
- **Medidas de Seguridad:** Utilizar técnicas de cifrado y seguridad para proteger los datos almacenados en el dispositivo del usuario.

Seguridad en la Comunicación

- **Objetivo:** Garantizar la seguridad de las comunicaciones entre la aplicación y el servidor, si corresponde.
- **Medidas de Seguridad:** Utilizar conexiones seguras (HTTPS) para cifrar la transferencia de datos entre la aplicación y el servidor.

Autenticación y Autorización

- **Objetivo:** Implementar un sistema de autenticación seguro para controlar el acceso a la aplicación.
- **Medidas de Seguridad:** Requerir que los usuarios se autentifiquen antes de acceder a la aplicación y sus funciones. Implementar controles de autorización para restringir el acceso no autorizado.

Aplicación de Registro de Empleados (App 2) y Página Web

Autenticación y Autorización

- Objetivo: Garantizar que solo los empleados autorizados puedan acceder a la aplicación y a las gráficas.
- Medidas de Seguridad: Implementar un sistema de autenticación y autorización sólido. Verificar la identidad de los usuarios y limitar el acceso a las funciones de acuerdo con sus roles y privilegios.

Protección contra ataques de inyección

- Objetivo: Evitar la inyección de código malicioso en formularios y aplicaciones.
- Medidas de Seguridad: Validar y filtrar cuidadosamente los datos de entrada de los usuarios para prevenir ataques de inyección, como SQL Injection o Cross-Site Scripting (XSS).

Monitorización de la Seguridad

- Objetivo: Detectar actividades sospechosas o intentos de acceso no autorizado.
- Medidas de Seguridad: Implementar un sistema de registro y monitorización de seguridad para identificar y responder a eventos de seguridad.

Protección contra Fuerza Bruta

- Objetivo: Prevenir ataques de fuerza bruta y denegación de servicio.
- Medidas de Seguridad: Implementar mecanismos para limitar el número de intentos de inicio de sesión y bloquear cuentas después de varios intentos fallidos.

Actualizaciones y Parches

- Objetivo: Mantener las aplicaciones y sistemas actualizados con correcciones de seguridad.
- Medidas de Seguridad: Realizar actualizaciones regulares y aplicar los últimos parches de seguridad para protegerse contra vulnerabilidades conocidas.

Protección de Datos

- Objetivo: Cumplir con las regulaciones de protección de datos aplicables.
- Medidas de Seguridad: Asegurarse de que se cumplan las regulaciones de protección de datos, como GDPR, para proteger la privacidad de los usuarios.

Evaluación de Vulnerabilidades

- Objetivo: Identificar y solucionar posibles vulnerabilidades.
- Medidas de Seguridad: Realizar pruebas de penetración y evaluaciones de seguridad para detectar y abordar posibles vulnerabilidades.

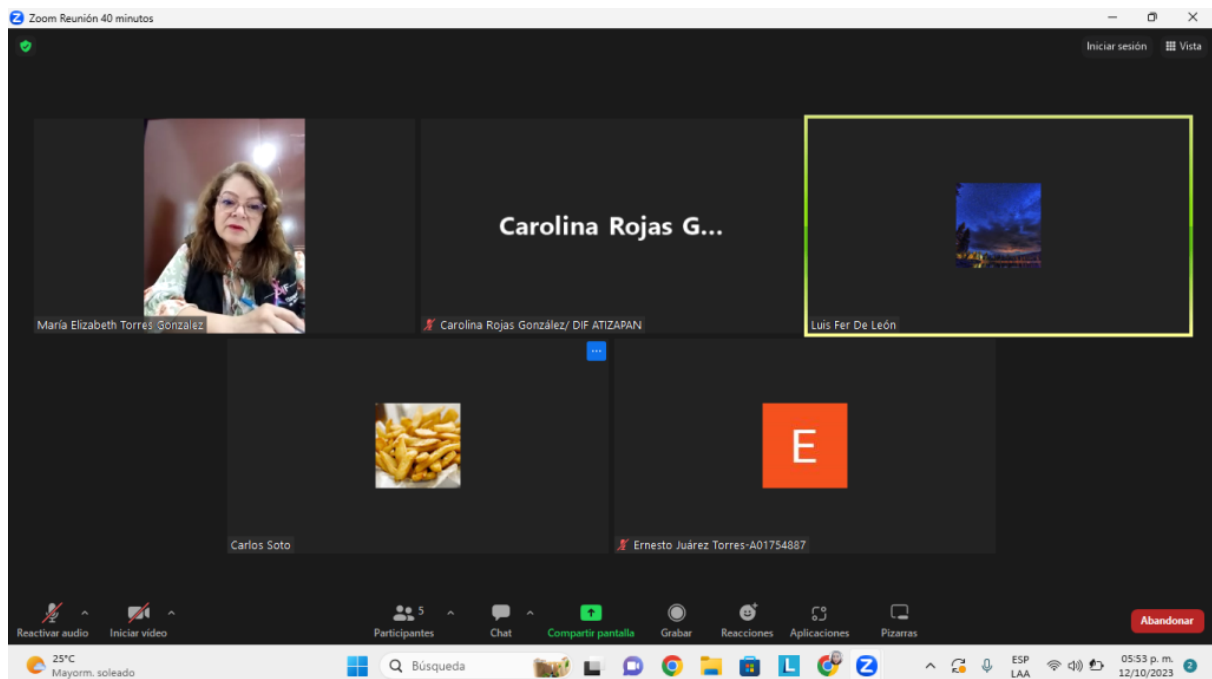
Formación de Empleados

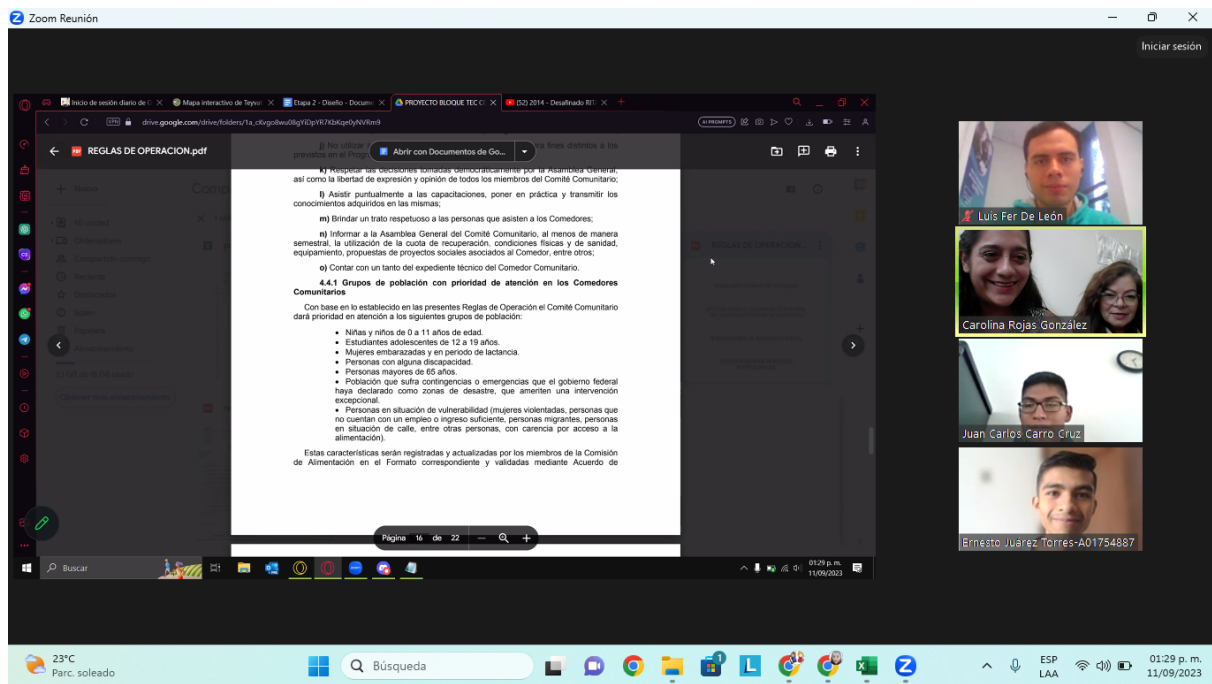
- Objetivo: Educar a los empleados y usuarios sobre prácticas de seguridad.
- Medidas de Seguridad: Proporcionar formación sobre la creación de contraseñas seguras, la detección de correos electrónicos de phishing y las mejores prácticas de seguridad.

Planes de Respuesta a Incidentes

- Objetivo: Estar preparado en caso de una brecha de seguridad.
- Medidas de Seguridad: Desarrollar planes de respuesta a incidentes para abordar eficazmente cualquier incidente de seguridad que pueda ocurrir.

Reuniones con el cliente





https://drive.google.com/file/d/1P89UupOkM4wetwTmU_mko-qvxScOXYKS/view

Reuniones con el equipo de desarrollo



Etapas 4

Plan de Pruebas

Objetivo: El plan de pruebas tiene como objetivo verificar exhaustivamente el correcto funcionamiento de las tres partes del sistema (página web para superadministrador, aplicación para administrador de comedor y aplicación para usuarios finales) y asegurarse de que interactúen de manera sin problemas.

Alcance: Todas las funcionalidades y características de las tres partes del sistema serán sometidas a pruebas para garantizar que cumplan con los requisitos y expectativas del proyecto.

Herramientas de Prueba:

Pruebas Unitarias con Kotlin.

Postman para pruebas de API.

Kotlin para desarrollo de aplicaciones móviles.

Herramientas y frameworks específicos para pruebas de integración de sistemas.

Datos de Prueba:

Casos de prueba positivos:

Datos válidos que representan situaciones donde se espera un resultado exitoso.

Casos de prueba negativos:

Ejemplos de datos inválidos que representen situaciones donde se espera un resultado de error. Por ejemplo, intentos de registro con direcciones de correo electrónico inválidas.

Datos límite:

Ejemplos de datos que están en el límite de lo que se espera que el sistema pueda manejar. Por ejemplo, si hay un campo de texto con un límite de 50 caracteres, incluye casos con 50 caracteres exactamente.

Datos nulos o vacíos:

Ejemplos que representen cómo el sistema maneja la ausencia de datos. Por ejemplo, si un campo es obligatorio, incluye casos donde el campo está vacío.

Escenarios de pruebas alfa y de regresión:

Escenarios alfa:

Datos ficticios pero realistas que reflejan el uso esperado del sistema por parte de los usuarios finales. Estos datos deben simular el ambiente real de uso.

Escenarios de seguridad:

Incluye datos que evalúen cómo el sistema responde a diferentes niveles de amenaza, simulando intentos de intrusión y pruebas de seguridad.

Casos de prueba de regresión:

Conjuntos de datos que verifiquen que las actualizaciones o cambios recientes no hayan introducido nuevos errores en el sistema.

Datos de Prueba:

3. Estrategia de Pruebas

Pruebas de Unidad

Probar los componentes de cada aplicación para ver quienes cumplen con las funciones específicas a las que están relacionadas

Pruebas de Integración

Verificar que el las partes del sistema funcionen correctamente

Pruebas de Usabilidad

Pruebas alfa en las que se probará el funcionamiento correcto de la aplicación.

Pruebas de Seguridad.

Mantener la integridad de los datos segura y con la privacidad adecuada al momento de usarlos, enviarlos y almacenarlos.

Casos de Prueba:

Página Web para Superadministrador:

Caso de prueba positivo - Inicio de Sesión:

Acción: Intentar iniciar sesión con credenciales válidas.

Resultado esperado: El administrador accede al panel de administración.

Caso de prueba negativo - Inicio de Sesión:

Acción: Intentar iniciar sesión con credenciales inválidas.

Resultado esperado: El sistema muestra un mensaje de error indicando credenciales incorrectas.

Caso de prueba - Crear Nuevo Comedor:

Acción: Crear un nuevo comedor desde el panel de administración.

Resultado esperado: El comedor se registra correctamente en el sistema.

Aplicación para Administrador de Comedor:

APP COMEDOR

Caso de prueba-Registro de Comensal

Acción: Registrar a una persona para acceder a alimentos.

Resultado esperado: La persona queda registrada en el sistema con la opción de acceso a alimentos.

Caso de prueba - Registro de Comida Donada:

Acción: Registrar una comida como donada desde la aplicación.

Resultado esperado: La comida queda marcada como donada en el sistema.

Aplicación para Usuarios Finales

Caso de prueba - Registro de condición de la persona

Acción: registrar: la condición de la persona será asignada con un spinner que selecciona una condición

Resultado esperado: La condición queda registrada al pulsar el botón

APP Comensal

Caso de prueba positivo - Registro de Usuario Final:

Acción: Un usuario final se registra y proporciona sus datos.

Resultado esperado: El usuario final queda registrado en el sistema y se genera un código QR asociado a su perfil.

Caso de prueba - Escaneo de Código QR:

Acción: El administrador de comedor escanea el código QR del usuario final.

Resultado esperado: El administrador tiene acceso a la información del usuario y puede proporcionar alimentos.

RTM (Requirement Traceability Matrix)

Matriz de Trazabilidad

Resultado de las pruebas

Las pruebas hechas en la matriz de trazabilidad son positivas sin embargo pruebas de usabilidad y de integración con las demás partes del sistema son erróneas y son críticas de corregir.

Informe y cierre de pruebas

En la revisión de las pruebas podemos considerar que el proyecto está funcionando a un 70 por ciento ya que las pruebas unitarias que se han hecho demuestran que las partes del sistema están funcionando además de drivers y stubs para comprobación, únicamente haría falta la interconexión correcta entre los mismos para el manejo de los datos.

Etapas Finales

Capacitación:

La capacitación en Dif+ App es sumamente importante, ya que de este modo, los administradores y los clientes podrán hacer uso correcto del sistema.

1. Objetivo: Familiarizar a los administradores con todo el sistema de Dif+ App

2. Audiencia Objetivo:
 - a. Comensales que deseen comer en un comedor comunitario
 - b. Ayudantes que deseen ayudar en el comedor comunitario
 - c. Administradores de comedor
3. Metodologías de capacitación
 - a. Manejo de bases de datos usando el motor MariaDB (Con comandos para evitar algún descuido o error de eliminación)
 - b. Manejo de Python, así como de Flask
 - c. Manejo básico de HTML y CSS para cualquier cambio de diseño y/o presentación.
 - d. Personalización de actividades con Kotlin y Android Studio
4. Duración de capacitación: La duración de la capacitación podría durar entre 3 a 5 días máximo. Sin embargo, dependerá de varios factores, tales como la experiencia del usuario, requisitos de cada grupo de usuarios, etc.
5. Recursos: Mientras que muchos de los recursos se encuentran actualmente en YouTube, existirán manuales de usuario e instalación anexados en PDF. También, existe un soporte técnico directamente relacionado con el equipo de desarrollo de Dif+ App.

Aportaciones Individuales

- **Luis:** Mi contribución al proyecto se centró en el desarrollo del back end que sustenta tanto la aplicación Dif+ App Comensal como la aplicación Dif+ App Empleado. Esto incluye la gestión de bases de datos, el procesamiento de datos y la lógica de negocio que permite la comunicación efectiva entre las aplicaciones y los servidores. Trabajé en la implementación de medidas de seguridad sólidas para proteger la integridad y la confidencialidad de los datos. Además, aseguré que el sistema fuera escalable y eficiente. Mi contribución al back end representa aproximadamente el 25% del proyecto.
- **Juan:** Mi contribución al proyecto se centra en el desarrollo de la aplicación Dif+ App Comedor. Esta aplicación es crucial para permitir que los empleados gestionen el sistema y accedan a información importante tal es el caso del registro de los comensales y el envío de reportes del mismo comedor ya sea para advertir una amenaza o una actualización del inventario. También acordar reunión con el DIF de Atizapán para tratar temas acerca de los elementos de la aplicación y cómo deberían verse. Trabajé en Android Studio para crear una aplicación eficiente y segura que proporciona a los empleados las herramientas necesarias para su trabajo. También me aseguré de que se siguieran las mejores prácticas de seguridad para proteger los datos y garantizar que solo los empleados autorizados tengan acceso a ciertas funciones.
- **Carlos:** Mi contribución al proyecto consistió en el desarrollo de una página web que brinda acceso y funcionalidades a través de navegadores web. Esta página web es

esencial para garantizar que el DIF pueda interactuar con los empleados y comensales de manera eficiente. Desarrollé la interfaz de usuario, la conectividad con la base de datos y aseguré que la página web cumpliera con los estándares de seguridad necesarios para proteger la información. La página web representa aproximadamente el 25% del proyecto.

- **Ernesto:** Nuestra aplicación, Dif+ App Comensal, es un componente clave de nuestro proyecto. Como parte del equipo, mi contribución se centró en su desarrollo. Utilicé Android Studio para crear una interfaz de usuario intuitiva y funcional que permite a los comensales acceder fácilmente a nuestros servicios. Además, el uso de datos es eficiente para el manejo de datos personales. Esto incluyó la validación del CURP y la implementación de una segunda pantalla por si es de que el. El desarrollo de esta aplicación representa aproximadamente el 25% de nuestro proyecto.

Link al video

[https://drive.google.com/drive/folders/1L3zS6aqfKENS_ak7sifRPwiXNgIH
Aw15](https://drive.google.com/drive/folders/1L3zS6aqfKENS_ak7sifRPwiXNgIHAw15)