



Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Estado de México

Escuela de Ingeniería y Ciencias

TC2007B.402

Integración de seguridad informática en redes y sistemas de software

Evidencia 1:

Documento de la solución del reto

Alumnos:

Alan Alcántara Ávila - A01753505

Diego Manjarrez Viveros - A01753486

Andrés Iván Rodríguez Méndez - A01754650

Carlos Alberto Sánchez Calderón - A01747433

Aldehil de Jesús Sánchez Hernández - A01748442

Profesores:

Humberto Cárdenas Anaya

Marco Antonio González Galicia

Mauricio Martínez Arias

Roberto Martínez Román

Fecha de entrega:

22/10/2023

Índice

Índice	2
Etapas	3
Problemática	3
Requerimientos funcionales	3
Requerimientos no funcionales	4
Casos de uso	5
Diagrama	5
Casos de uso extendidos	5
Pensamiento crítico	10
Estándares de administración de proyectos	10
Variables de desempeño	11
Alcances del proyecto	11
Entregables del proyecto	12
Calendarización del proyecto	12
Estimación del esfuerzo del proyecto	12
Análisis de riesgos	13
Prototipo	14
Aplicación	14
Página web	15
Etapas	16
Diagramas de diseño	16
Diagrama del diseño de la base de datos	16
Diagrama de la arquitectura de la app	17
Diagrama de clases de la app	17
Diseño de las interfaces de usuario	18
Aplicación	18
Página web	19
Integración de seguridad en sistemas computacionales	20
Etapas	21
Repositorio	21
Identificación de ataques informáticos	21
Métodos de Infiltración	23
Métodos de protección de ataques informáticos	23
Etapas	25
Matriz de trazabilidad	25
Reporte de pruebas con resumen	25
Reporte de incidentes	25
Etapas	26
Manuales	26
Manuales de usuario	26
Manual de administrador	26
Manual de instalación	26

Etapa 1

Problemática

En el contexto actual, la administración de los comedores comunitarios en el DIF de Atizapán se enfrenta a una serie de desafíos que dificultan su eficiencia y operatividad. Entre estos desafíos destacan la falta de un sistema integral de gestión, lo que lleva a una organización manual y propensa a errores en la asignación de recursos, seguimiento de menús, registro de beneficiarios y control de inventario. Además, la comunicación entre los diferentes niveles de la administración y la comunidad se ve limitada, lo que impacta en la capacidad de adaptar los servicios a las necesidades cambiantes de los usuarios. Estas problemáticas convergen en la necesidad apremiante de una solución tecnológica que simplifique y optimice la administración de los comedores comunitarios, permitiendo así brindar un apoyo más efectivo y oportuno a quienes dependen de estos servicios vitales.

Requerimientos funcionales

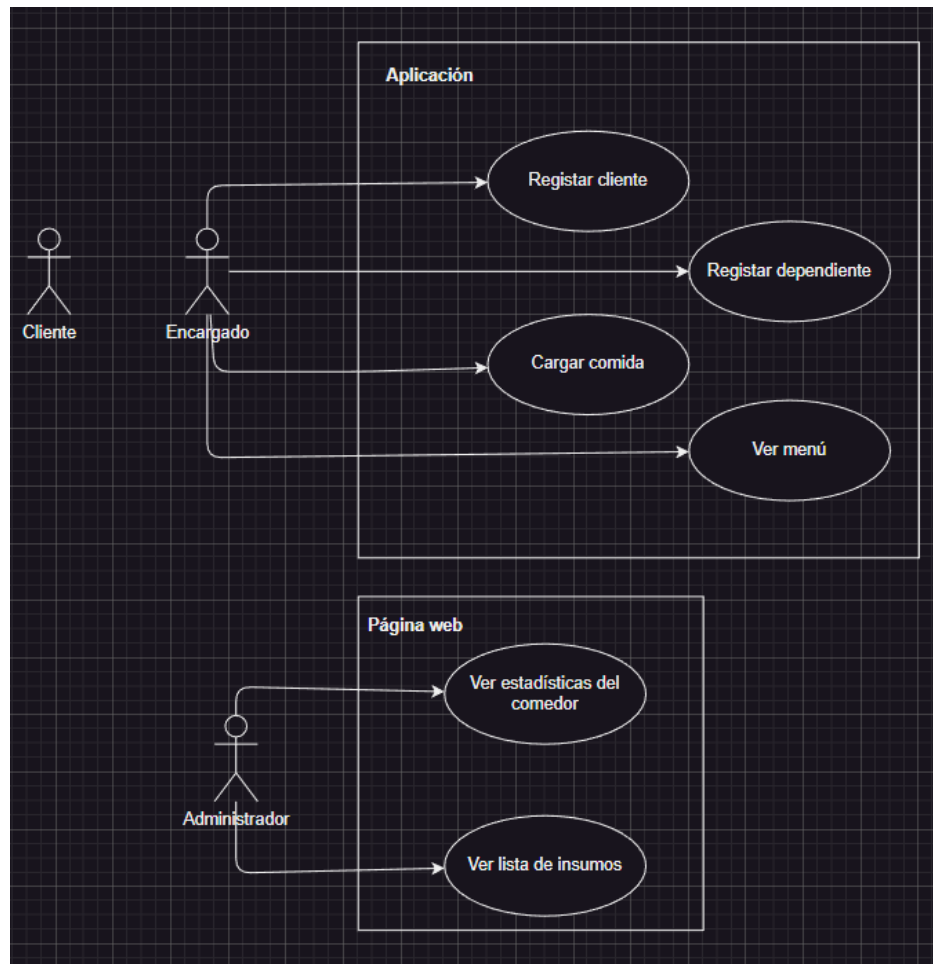
- El sistema permite almacenar datos personales del usuario
- El encargado será capaz de registrar a los usuarios y guardar su información
- El sistema permite crear perfiles de usuario para cada CURP
- El encargado podrá ingresar a los perfiles de usuario y verificar la información previamente registrada
- El sistema permite registrar dependientes en los perfiles de usuario que lo requieran
- El encargado podrá dar de alta el menú diario
- El sistema permite registrar pedidos de usuarios junto con sus dependientes
- El encargado podrá analizar los datos que se almacenan en la aplicación
- El sistema permitirá mostrar gráficas con los pedidos registrados

Requerimientos no funcionales

- Disponibilidad: La aplicación estará disponible en dispositivos Android para cualquier comedor. Esto se mediría contando la cantidad de comedores que usan la aplicación.
- Facilidad de uso: El sistema debe ser fácil de usar y de comprender. Mediante las horas que le toma a un usuario usar la aplicación podremos medir este requerimiento.
- Responsividad: La página web y aplicación deben ser responsivas, lo cual mediremos en base al rango de píxeles usados tanto en pantallas pequeñas como en dispositivos con mayor cantidad de pixeles.
- Seguridad: La base de datos debe estar protegida de cualquier acceso no autorizado. Para ello protegeremos nuestra base de datos con una contraseña encriptada.
- Proveedor de la nube: Los servidores en la nube estarán montados en AWS
- Fiabilidad: El sistema debe de ser confiable y cumplir con los requisitos del usuario. Esto se medirá en base que el 90% del tiempo no tendremos errores críticos que afecten la implementación del sistema.

Casos de uso

Diagrama



Casos de uso extendidos

Caso de uso (Registrar usuario)

Actores	Encargado
Descripción	El encargado recibe a un cliente en el comedor que no se encuentra en el sistema por lo que requiere hacer su registro.

Escenario principal	El encargado ingresa los datos del cliente en la aplicación para poder registrarlo y darle su comida.
Excepciones	La aplicación no puede ser usada por falta de dispositivos. La comida es donada.
Precondiciones	Conexión a internet Dispositivo android para ingresar a la aplicación
Diagrama de secuencia:	
Actores	Sistema
1. El encargado ingresa a la aplicación.	
2. El encargado se va a la sección de registro para ingresar los datos del cliente.	3. El sistema guarda los datos del cliente y crea su perfil en el registro.
4. El encargado puede acceder al perfil y se le puede cobrar al cliente.	
Casos alternativos	

Antes del paso 2. El cliente ya está registrado en el sistema.

En el paso 2. El cliente no quiere dar su información o le faltan datos, por lo que no podrá ser registrado

Caso de uso (Registrar comida)

Actores	Encargado
Descripción	El encargado recibe a un cliente en el comedor que ya está en el registro por lo que solo le asigna una comida
Escenario principal	El encargado ingresa al perfil del cliente en la aplicación y le asigna una comida comprada.
Excepciones	La aplicación no puede ser usada por falta de dispositivos. La comida es donada.
Precondiciones	Conexión a internet Dispositivo android para ingresar a la aplicación
Diagrama de secuencia:	
Actores	Sistema

1. El encargado ingresa a la aplicación.	
2. El encargado busca en la lista de registro el nombre del cliente e ingresa al perfil.	3. El sistema muestra los datos del cliente y permite cargarle una comida al cliente.
4. El encargado le cobra al cliente una comida y la carga en la aplicación.	5. El sistema guarda la comida cobrada en la base de datos.
Casos alternativos	
<p>En el paso 2. El cliente no está registrado en el sistema, por lo que debe de realizar el registro primero.</p> <p>En el paso 4. El cliente quiere otra comida para otra persona dependiente por lo que debe realizar el registro de esa persona previamente.</p>	

Caso de uso (Registrar dependiente)

Actores	Encargado
Descripción	El encargado recibe a un cliente en el comedor que está registrado pero quiere comida para otra persona por lo que debe hacer su registro
Escenario principal	El encargado ingresa los datos del dependiente en la aplicación para poder registrarlo y darle su comida.

Excepciones	<p>La aplicación no puede ser usada por falta de dispositivos.</p> <p>La comida es donada.</p>
Precondiciones	<p>Conexión a internet</p> <p>Dispositivo android para ingresar a la aplicación</p>
Diagrama de secuencia:	
Actores	Sistema
1. El encargado ingresa a la aplicación.	
2. El encargado ingresa al perfil del cliente previamente registrado.	3. El sistema muestra los datos del cliente y permite asignarle un dependiente.
4. El encargado ingresa los datos del dependiente en la aplicación.	5. El sistema guarda los datos ingresados en la base de datos y asigna esa persona como dependiente del cliente en su perfil.
6. El encargado puede acceder al perfil del cliente y se le puede cargar su comida y la de su dependiente.	7. El sistema guarda las comidas cobradas en la base de datos.

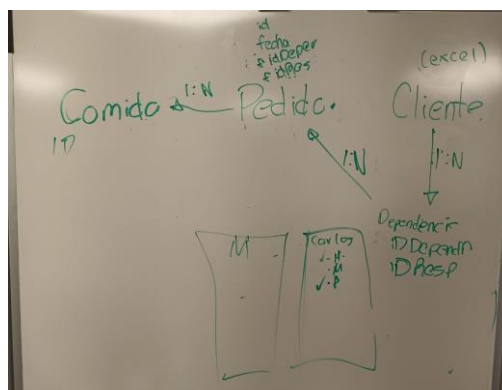
Casos alternativos

Después del paso 5. El cliente quiere registrar a otro dependiente por lo que se repite el proceso desde el paso 2.

En el paso 4. El cliente no quiere dar información o le faltan datos del dependiente, por lo que no podrá ser registrado y no se le podrán dar más de 1 comida.

Pensamiento crítico

Después de la reunión con el socio-formador, en equipo hicimos una lluvia de ideas en la cual revisamos la problemática y con ello identificamos los requerimientos funcionales y no funcionales del proyecto. También con ayuda de un pizarrón debatimos sobre el diseño de la base de datos y sobre donde la montaremos, así como que servicio en la nube ocuparemos, por último discutimos el nombre y como seria la vista de la aplicación y como estaba organizada la interfaz de la aplicación.



Estándares de administración de proyectos

Nosotros seleccionamos el método SCRUM ya que es el que más se adapta a nuestra manera de trabajo y a como queremos que funcione nuestro desarrollo. Consideramos que trabajar por sprints es la forma más rápida y eficaz en la que podemos ir implementando los requerimientos, por otra parte seleccionamos SCRUM ya que podemos ir regresando a los requerimientos para hacer cambios o agregar más si nosotros creemos que es necesario, mientras probamos código.

Variables de desempeño

- Conexión de internet
- Dispositivo con Android versión 7 o posterior
- Equipo de mantenimiento
- Equipo de desarrollo
- computadoras
- Servicios en la nube
- Servidores

Alcances del proyecto

El alcance del proyecto incluye:

- Una aplicación móvil para registrar clientes nuevos, crear y registrar sus pedidos.
- Una página web que permite monitorear los datos recolectados de los diferentes comedores, aplicando diferentes filtros.
- Una base de datos apta para el completo funcionamiento de la aplicación y la monitorización de datos
- Documentación sobre el manejo de la app para los usuarios y la monitorización de datos para los administradores.

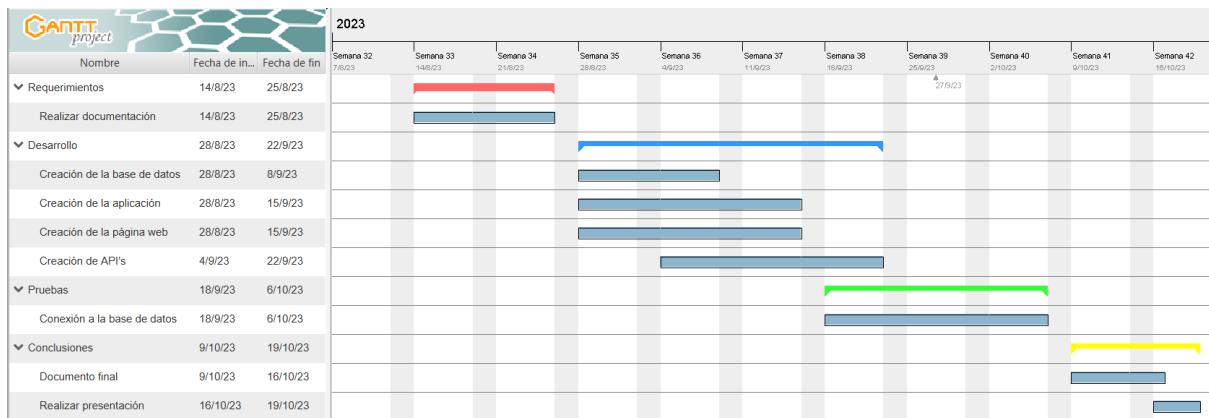
El proyecto no incluye:

- Las licencias para el funcionamiento total de la aplicación, por ejemplo la de la base de datos y la de algunos componentes de la monitorización de datos.

Entregables del proyecto

- Aplicación funcional desarrollada en Android Studio
- Página web funcional desarrollada con HTML y Javascript
- Base de datos SQL
- Documentación completa del proyecto

Calendarización del proyecto



Estimación del esfuerzo del proyecto

Se utilizará el modelo de FPA, que divide en puntos de funcionamiento el sistema y el tiempo promedio que toma hacer estos módulos y los multiplica para obtener el aproximado en tiempo que tomaría desarrollar el proyecto. En adición se debe de considerar diversos factores de complejidad, entre los que se encuentran la experiencia, la tecnología utilizada, los requisitos del cliente y la complejidad del software. Este factor se considera de 1.0 siendo para proyectos simples y 1.5 para proyectos complejos.

$$\text{Puntos de función ajustados} = \text{Puntos de función} * \text{Factor de ajuste}$$

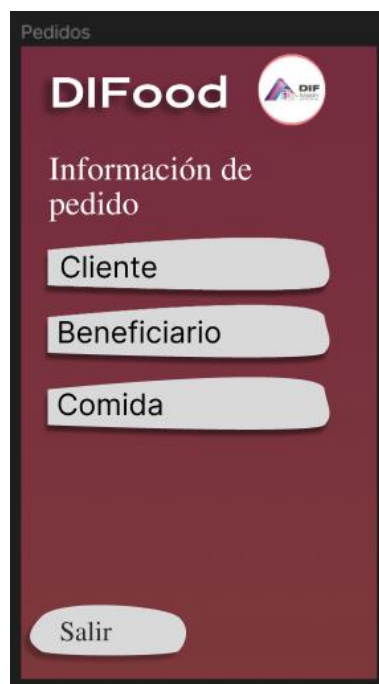
Análisis de riesgos

		Impacto		
		Bajo (1)	Medio (2)	Alto (3)
Probabilidad	Bajo (1)	Inicio de una pandemia -> 1	Se pierda la computadora de un integrante -> 2	Falla crítica en Android Studio -> 3
	Medio (2)	Incompatibilidad de tecnologías de desarrollo -> 2	Falla en la integración del front con el back -> 4	Se pierda el repositorio del proyecto-> 6
	Alto (3)	Un integrante trabaje menos de lo esperado ->3 Cambio de administración en el DIF -> 3	Desacuerdos en problemas del desarrollo -> 6	

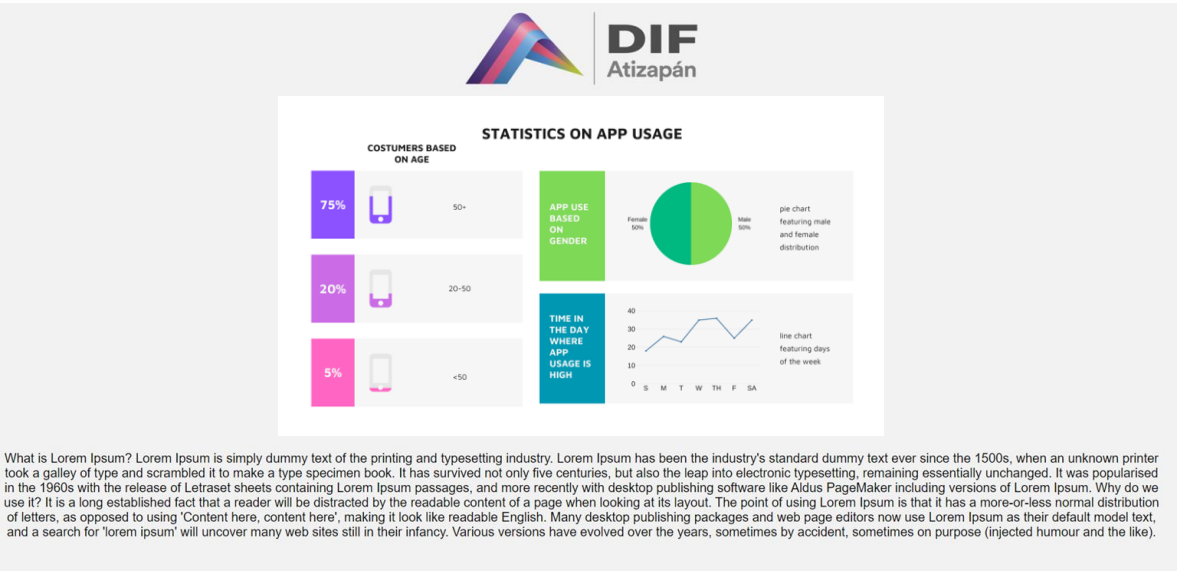
Prototipo

Aplicación

<https://www.figma.com/file/6xuoXe4BaJ5QQAgto0Q1ty/DiFood?type=design&node-id=0%3A1&mode=design&t=Zi3fLG9S1ZI9ixBd-1>



Página web



Etapa 2

Diagramas de diseño

Diagrama del diseño de la base de datos

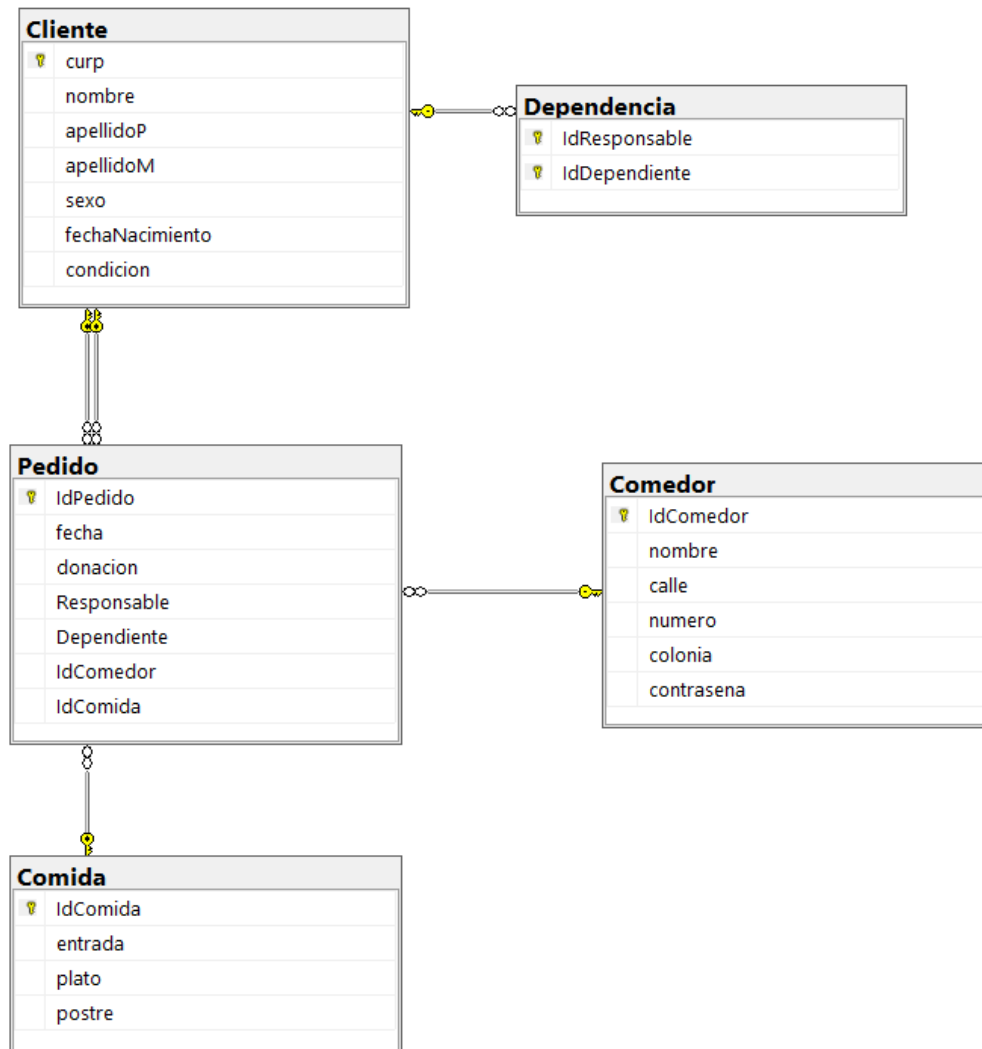


Diagrama de la arquitectura de la app

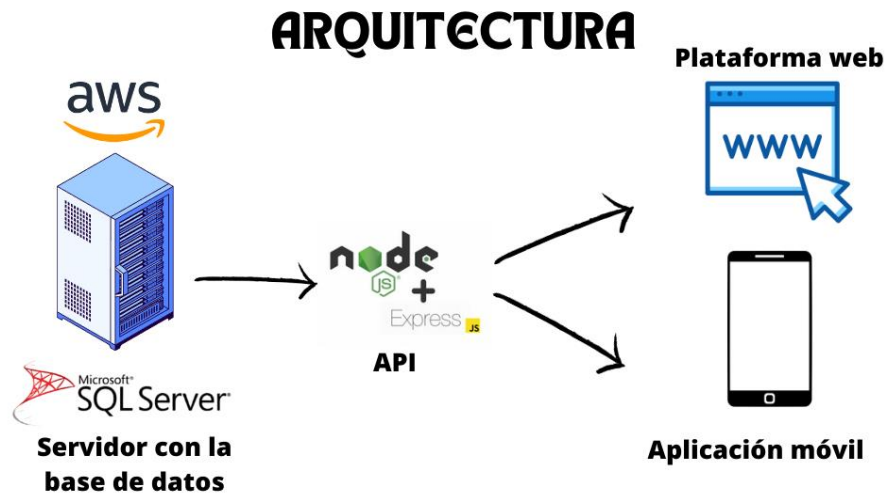
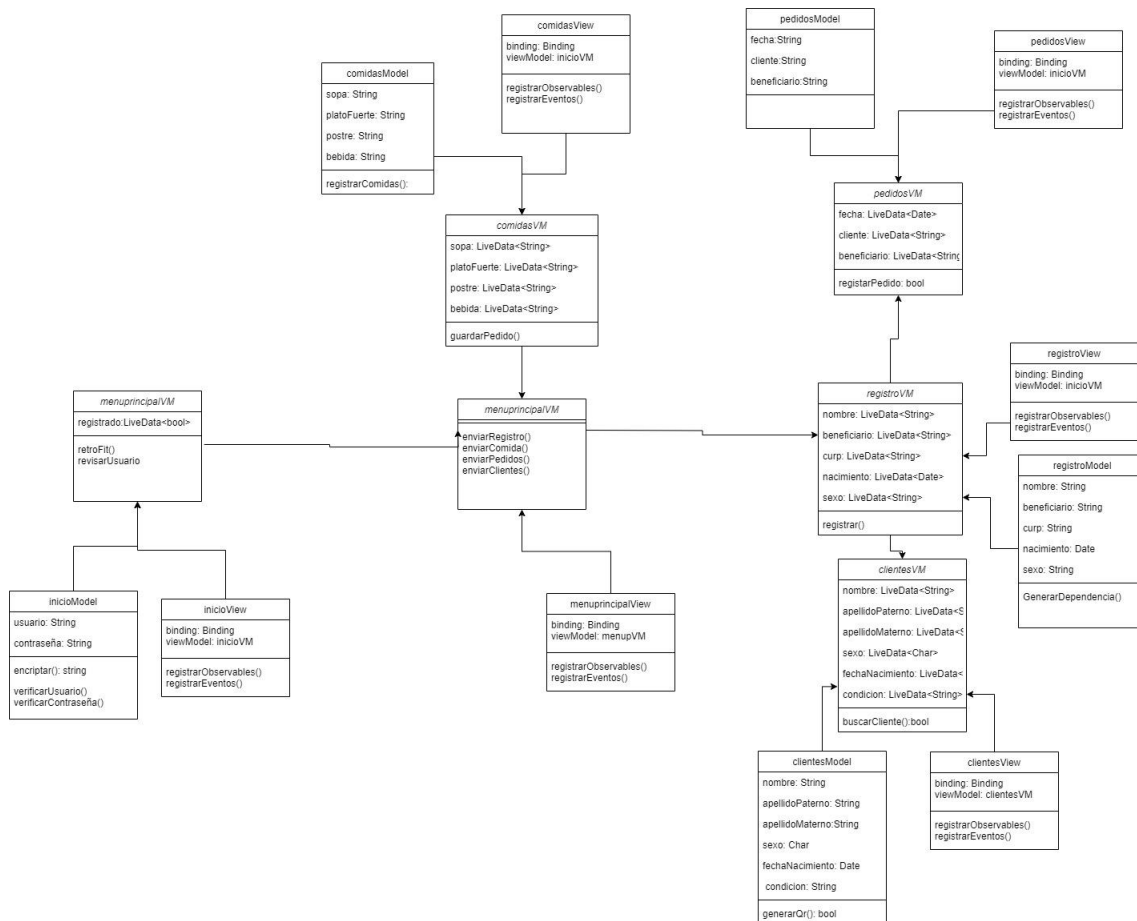


Diagrama de clases de la app

<https://drive.google.com/file/d/1JwansdTWp49B6fdrbh2Axmbnq0Y2DUha/view?usp=sharing>



Diseño de las interfaces de usuario

Aplicación

The image displays six mobile application screens for 'DIFood', arranged in two rows of three. Each screen features a dark red background with a white 'DIF' logo in the top right corner.

- InicioDeSesion:** Features the 'DIFood' title, a login form with fields for 'Nombre de Sucursal....' and 'Contraseña.....', and an 'Iniciar Sesión' button.
- MenuPrincipal:** Displays a central menu with five options: 'Hacer pedido', 'Registrar cliente', 'Ver clientes', 'Registrar comida', and 'Salir'.
- RegistroCliente:** Shows a 'Registrar cliente' form with fields for 'Nombre', 'Beneficiario', 'CURP', 'Sexo', and 'Edad', followed by a 'Salir' button.
- RegistrarPedido:** Prompts the user to 'Ingresa el menú del día de hoy' with input fields for 'Sopa', 'Plato Fuerte', 'Postre', and 'Bebida', and a 'Registrar' button.
- Pedidos:** Displays 'Información de pedido' with fields for 'Cliente' and 'Beneficiarios' (with a dropdown arrow), and a 'Salir' button.
- Clientes:** Shows a 'Clientes' list with a search icon, a list of client entries, and a 'Salir' button.

Página web

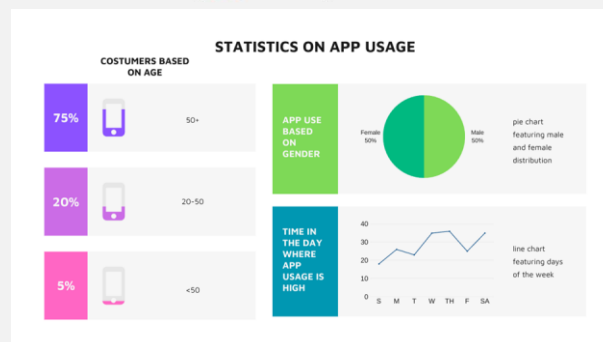
Login Administración Monitor de Comedores

Usuario:

Contraseña:

Ingresar

Hecho por Tec CEM



What is Lorem Ipsum? Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum. Why do we use it? It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy. Various versions have evolved over the years, sometimes by accident, sometimes on purpose (injected humour and the like).

Integración de seguridad en sistemas computacionales

- Separación de funcionalidades en dos aplicaciones para no tener información innecesaria en lugares que no deberían tener acceso.
- Aplicar un algoritmo de hash a las contraseñas que se almacenan en la base de datos, de modo que si llega a haber filtraciones, no se pueda obtener la contraseña.
- Acceso a la base de datos solo con contraseña y usuario de administrador.
- Acceso restringido a la aplicación para los usuarios.
- Tipo de input password en la aplicación para que no se pueda observar por alguien más.
- Obtener el certificado https para no tener el contenido como texto plano.
- Implementación del sistema TLS en nuestra aplicación.

Etapa 3

Repositorio

<https://github.com/Dmanjav/retoDIF>

- Link a la aplicación del comedor:
<https://github.com/Dmanjav/retoDIF/tree/main/aplicacionComedor>
- Link a la aplicación del cliente:
<https://github.com/Dmanjav/retoDIF/tree/main/DifoodAme>
- Link al API y a página web:
<https://github.com/Dmanjav/retoDIF/tree/main/web>

Identificación de ataques informáticos

Actualmente, hay múltiples ataques y con diferentes objetivos, entre los que se encuentran:

- **Ataques de acceso no autorizado:** El objetivo de este tipo de ataques es obtener acceso a un sistema o red sin autorización.
- **Ataques de robo de datos:** El objetivo de este tipo de ataques es robar información confidencial, como datos personales, contraseñas o información financiera.
- **Ataques de denegación de servicio (DoS):** El objetivo de este tipo de ataques es sobrecargar un sistema o red para impedir que funcione correctamente.
- **Ataques de malware:** El objetivo de este tipo de ataques es instalar software malicioso en un sistema para dañarlo o robar información.
- **Ataques de ciberespionaje:** El objetivo de este tipo de ataques es recopilar información confidencial sobre una persona o organización.
- **Ataques de guerra cibernética:** El objetivo de este tipo de ataques es causar daño o destrucción a un sistema o red.

Para realizar esos ataques se encuentran diferentes tipos de técnicas, cada una de estas tiene su forma de parar el ataque:

- Spyware: Espía todo, desde las teclas, información, cambia los sistemas de seguridad de la computadora, normalmente viene con Troyanos.
- Adware: Muestra anuncios, normalmente viene en la web y sirve para spamear anuncios.
- Backdoor: Sirve para conseguir acceso remoto a los sistemas y son complicados de detectar
- Ransomware: Atrapa tu información y no la descripta hasta que hagas un pago, normalmente viene con phishing y descargas de software raras.
- Scareware: Te espantan para que hagas lo que dice la computadora y te termina instalando más virus de los que ya tenías.
- Rootkit: Modifica el software de los dispositivos para dejarles una puerta trasera, muy complicada de detectar y la solución es borrar toda la computadora.
- Virus: Se descargan y se replican en las computadoras, algunos solo muestran una imagen pero otros pueden llegar a borrar y modificar archivos. Normalmente vienen en discos, USB, etc.
- Troyanos: Sirva para meter software adicional que puede hacer más daño, se ven certificados y todo pero solo son apariencias, no se replica a sí mismo.
- Gusanos: Se pasa de computadora a computadora, no requiere interacción del usuario como los virus, corre solito. Se replica a sí mismo sirven para vulnerar dispositivos dando lugar a otras cosas.

Métodos de Infiltración

- **DoS:** Interrumpe las conexiones de servicios, de usuarios, de aplicaciones. Se suele ver cuando hay mucho tráfico que no puede ser manejado, por lo que crashean los dispositivos, igual mandar paquetes incorrectos crashean la computadora.
- **DDoS:** Igual que el DoS pero viene de múltiples fuentes, llamados zombies, infectan a otros dispositivos.
- **Botnet:** Son muchas computadoras infectadas que sirven para hacer DDoS, spam, o incluso usarlas como fuerza bruta para obtener passwords de todo.
- **On-Path**

Sirven para interceptar comunicaciones entre dispositivos, uno es el MITM y otro MITMO

- **MITM:** se mete en el dispositivo del usuario y captura información directa de este antes de mandarla al servidor.
- **MITMO:** se mete en el dispositivo y accede a información delicada, como son la verificación de dos pasos y se la manda a los atacantes.
- **SEO Poisoning:** Manipulación de los resultados de búsqueda de ciertos sitios para hacer que sean de los más visitados, con esto se puede aplicar la ing social para que la gente interactúe con estos sitios.
- **Advanced Persistent Threats:** Duran mucho, están bien financiados, y son bombas de tiempo que liberan malware personalizado hasta el momento deseado y se mantienen indetectables.

Métodos de protección de ataques informáticos

- **Contraseñas seguras:** Las contraseñas son la primera línea de defensa contra los ataques informáticos. Es importante crear contraseñas seguras que sean difíciles de adivinar. Las contraseñas seguras deben tener al menos 12 caracteres de longitud y deben incluir una combinación de letras, números y símbolos.
- **Software antivirus y antimalware:** El software antivirus y antimalware es esencial para proteger los sistemas informáticos de los virus, el malware y otras amenazas. Es importante mantener el software antivirus y antimalware actualizado para garantizar que esté protegido de las últimas amenazas.

- **Firewall:** Un firewall es un dispositivo de seguridad que controla el tráfico de red entrante y saliente. Los firewalls pueden ayudar a bloquear los ataques informáticos que intentan ingresar a un sistema a través de Internet.
- **Educación y concienciación:** Es importante educar a los empleados sobre las amenazas cibernéticas y cómo protegerse. Los empleados deben saber cómo identificar y evitar ataques informáticos.
- **Actualizaciones de software:** Los fabricantes de software suelen lanzar actualizaciones de seguridad para corregir vulnerabilidades que pueden ser explotadas por los atacantes. Es importante instalar las actualizaciones de software lo antes posible para mantener los sistemas informáticos protegidos.
- **Cifrado:** El cifrado puede ayudar a proteger los datos confidenciales de ser robados o utilizados por personas no autorizadas.
- **Seguridad de la nube:** Las empresas que utilizan servicios en la nube deben implementar medidas de seguridad para proteger sus datos y sistemas.
- **Seguridad física:** La seguridad física también es importante para proteger los sistemas informáticos y los datos. Las empresas deben implementar medidas de seguridad físicas, como control de acceso y cámaras de seguridad, para disuadir a los atacantes.

Etapa 4

Matriz de trazabilidad

<https://docs.google.com/spreadsheets/d/1pem2R2cwTgewkqvASWFLt1w8wgl1f-ad/edit?usp=sharing&ouid=114175151321062271111&rtpof=true&sd=true>

Reporte de pruebas con resumen

<https://docs.google.com/spreadsheets/d/1nbExlssUi0GVRm-iiin0SDoVvzwAxR1WiEVNTFozcix8/edit?usp=sharing>

Reporte de incidentes

https://docs.google.com/spreadsheets/d/1y8wYJELwHf5jXuS7TylsxwRWSmQIB_7ZicYZ-x1R8ul/edit?usp=sharing

Etapa 5

Manuales

Manuales de usuario

Manual de aplicación para los clientes

<https://docs.google.com/document/d/1kyC4Ee6vxk2DuEtTcNBcCDv6vVBsjSVpREVXKhApal0/edit?usp=sharing>

Manual de aplicación para encargados del comedor

https://docs.google.com/document/d/1BCrmvfLnaqZqY1kt2zY0Dr_gCrnPrR0Dmlk49zU68es/edit?usp=sharingv

Manual de administrador

https://docs.google.com/document/d/1UIKjMYBHgFnoAaOko_QIOGDYXZn5IZ6Ch4aXaAxyXIY/edit?usp=sharing

Manual de instalación

https://docs.google.com/document/d/1Yt509zITUGG0L9INoyvBavkdmV2j_eWxCDpj_c5461oE/edit?usp=sharing