Requerimientos de Seguridad

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

Introducción
Formalizar los requerimientos de seguridad establecidos para el desarrollo del proyecto el cual
deberá permitir la gestión de un servicio de buffet.

Requerimientos de seguridad			
N°	**Título**	**Descripción**	**Prioridad**
01	Mantener el software actualizado	Aplicar parches de seguridad y actualizaciones de software con regularidad	Media
02	Seguridad desde el diseño	La seguridad debe ser una consideración fundamental desde las primeras etapas del desarrollo	Media
03	Capacitación del personal	Asegurar que el equipo de desarrollo comprenda las mejores prácticas de seguridad	Media
04	Manejar las excepciones de forma segura para evitar que se revele información sensible	Evitar que se revele información sensible	Alta
05	Manejo de errores y excepciones	No mostrar mensajes de error que revelen información sensible al usuario final	Alta
06	Implementación de mecanismos de autenticación	Utilizar un mecanismo de autenticación robusto, como JWT	Alta
07	Manejo de sesiones	Invalidar las sesiones después de un período de inactividad	Media
08	No mostrar mensajes de error que revelen información sensible al usuario final	Utilizar mensajes de error descriptivos para ayudar al usuario a corregir los errores	Media
09	Crear la base de datos con los permisos de acceso mínimos necesarios	Crear la base de datos con los permisos de acceso mínimos necesarios	Media
10	Invalidar las sesiones después de un período de inactividad	Invalidar las sesiones después de un período de inactividad	Baja

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

11	Implementar un mecanismo de "token jwt" para proteger las acciones que modifican datos	Proteger las acciones que modifican datos	Alta
12	Manejo específico de rutas	Implementar reglas de validación para cada tipo de dato (longitud, formato, valores permitidos)	Media
13	Utilizar mensajes de error descriptivos para ayudar al usuario a corregir los errores	Ayudar al usuario a corregir los errores	Baja
14	Implementar reglas de validación para cada tipo de dato (longitud, formato, valores permitidos)	Validar todos los datos de entrada del usuario para prevenir ataques de scripting entre sitios (XSS), inyección de código y otros tipos de ataques	Media
15	Escribir código limpio, bien documentado y fácil de entender	Escribir código limpio, bien documentado y fácil de entender	Alta
16	Realizar pruebas de seguridad estáticas y dinámicas para detectar vulnerabilidades	Detectar vulnerabilidades	Alta
17	Implementar un proceso de revisión de código para asegurar la calidad del mismo	Asegurar la calidad del código	Alta
18	Eliminar los datos de prueba y scripts de desarrollo antes de la producción.	Eliminar los datos de prueba y scripts de desarrollo antes de la producción	Media

Modelado de amenazas				
Amenaza	**Descripción**	**Impacto**	**Probabilidad**	**Controles**
Inyección SQL	Un atacante podría obtener acceso no autorizado a la base de datos.	Alto	Medio	Usar parámetros para consultas SQL, validar entrada del usuario.
Cross-Site Scripting (XSS)	Un atacante podría ejecutar	Alto	Medio	Validar datos de entrada del usuario,

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

	scripts maliciosos en el navegador del usuario.			implementar reglas de validación.
Autenticación Insegura	Robo de contraseñas en caso de una violación de seguridad.	Alto	Alto	Almacenar contraseñas de forma segura, usar mecanismos de autenticación robustos.
Robo de Sesión	Un atacante podría hacerse pasar por un usuario legítimo.	Medio	Alto	Invalidar sesiones después de inactividad, usar tokens JWT para proteger acciones.
Exposición de Información Sensible	Mensajes de error podrían revelar información sensible.	Medio	Medio	Manejar excepciones de forma segura, no mostrar información sensible al usuario.
Ataques de Fuerza Bruta	Adivinación de contraseñas por parte de atacantes.	Medio	Alto	Implementar políticas de bloqueo de cuentas, usar contraseñas seguras.
Intercepción de Datos Sensibles	Los datos transmitidos podrían ser interceptados por un atacante.	Alto	Alto	Usar conexiones seguras HTTPS, implementar medidas de seguridad adicionales.
Manipulación de precios	Un atacante podría intentar manipular los precios de los productos en el sistema, ya sea reduciendo o aumentando los precios de los artículos.	Alto	Alto	Implementar controles de integridad en el lado del servidor para garantizar que los precios de los productos no puedan ser modificados sin autorización
Fuga de datos del cliente	Los datos personales y financieros de los clientes podrían ser objeto de robo o fuga.	Medio	Alto	Implementar medidas de seguridad robustas para proteger los datos del cliente, como el cifrado de

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

				datos sensibles, el uso de conexiones seguras HTTPS y el cumplimiento de estándares de seguridad de la industria, como el PCI DSS.
Ataques de denegación de servicio (DoS)	Un atacante intenta inundar el sistema con una gran cantidad de solicitudes maliciosas para sobrecargarlo y hacerlo inaccesible para los usuarios legítimos.	Medio	Medio	Configurar límites de tasa en las solicitudes de API para prevenir la sobrecarga del servidor.
Vulnerabilidades de terceros	Las vulnerabilidades en las bibliotecas de terceros utilizadas en el sistema podrían ser explotadas por los atacantes para comprometer la seguridad del sistema buffet.	Bajo	Medio	Mantener actualizadas todas las bibliotecas y frameworks de terceros, aplicar parches de seguridad de manera oportuna y realizar evaluaciones regulares de vulnerabilidades en el software utilizado.
Ataques de phishing dirigidos a empleados	Los empleados podrían ser blanco de ataques de phishing, donde los atacantes intentan engañarlos para que revelen información confidencial.	Medio	Medio	Implementar programas de concientización y capacitación en seguridad para los empleados, utilizar filtros de correo electrónico para detectar y bloquear correos electrónicos de phishing y establecer procedimientos para verificar la autenticidad de las solicitudes de información confidencial.

Requerimientos de Seguridad

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

Requerimiento	**Elemento**	**Fallo**	**Causa**	**Solución**
Gestionar Paquetes de Servicios	Crear Paquete	No se puede crear el paquete	Error al validar datos o guardar información	Implementar validaciones correctas y manejo de excepciones
			Datos incompletos	Mostrar mensaje de error indicando los campos faltantes
			Categoría o servicio no existe	Verificar la existencia de categorías y servicios
	Editar Paquete	No se puede editar el paquete	Error al cargar el paquete o guardar cambios	Verificar existencia del paquete y manejar excepciones
			Datos incorrectos	Mostrar mensaje de error indicando los datos inválidos
	Eliminar Paquete	No se puede eliminar el paquete	Paquete ligado a otros elementos	Implementar eliminación segura con verificación de dependencias
			Error al eliminar información	Manejar correctamente las excepciones al eliminar
Gestionar Categorías	Crear Categoría	No se puede crear la categoría	Error al validar nombre o guardar información	Implementar validaciones correctas y manejo de excepciones
			Nombre ya existe	Mostrar mensaje de error indicando nombre duplicado
	Editar Categoría	No se puede editar la categoría	Error al cargar la categoría o guardar cambios	Verificar existencia de la categoría y manejar excepciones
			Nombre ya existe	Mostrar mensaje de error indicando nombre

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

				duplicado
	Eliminar Categoría	No se puede eliminar la categoría	Categoría ligada a servicios o paquetes	Implementar eliminación segura con verificación de dependencias
			Error al eliminar información	Manejar correctamente las excepciones al eliminar
Gestionar Servicios	Crear Servicio	No se puede crear el servicio	Error al validar datos o guardar información	Implementar validaciones correctas y manejo de excepciones
			Datos incompletos	Mostrar mensaje de error indicando los campos faltantes
			Categoría no existe	Verificar la existencia de la categoría
	Editar Servicio	No se puede editar el servicio	Error al cargar el servicio o guardar cambios	Verificar existencia del servicio y manejar excepciones
			Datos incorrectos	Mostrar mensaje de error indicando los datos inválidos
	Eliminar Servicio	No se puede eliminar el servicio	Servicio ligado a paquetes o eventos	Implementar eliminación segura con verificación de dependencias
			Error al eliminar información	Manejar correctamente las excepciones al eliminar
Gestionar Usuarios	Crear Usuario	No se puede crear el usuario	Error al validar datos o guardar información	Implementar validaciones correctas y manejo de excepciones
			Datos incompletos	Mostrar mensaje de error indicando los campos faltantes

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

			Correo electrónico ya existe	Mostrar mensaje de error indicando correo electrónico duplicado
	Editar Usuario	No se puede editar el usuario	Error al cargar el usuario o guardar cambios	Verificar existencia del usuario y manejar excepciones
			Datos incorrectos	Mostrar mensaje de error indicando los datos inválidos
	Eliminar Usuario	No se puede eliminar el usuario	Usuario tiene información asociada	Implementar eliminación segura con verificación de relaciones
			Error al eliminar información	Manejar correctamente las excepciones al eliminar
Gestionar Personal	Crear Personal	No se puede crear el empleado	Error al validar datos o guardar información	Implementar validaciones correctas y manejo de excepciones
			Datos incompletos	Mostrar mensaje de error indicando los campos faltantes
			Rol no existe	Verificar la existencia del rol
	Editar Personal	No se puede editar el empleado	Error al cargar el empleado o guardar cambios	Verificar existencia del empleado y manejar excepciones
			Datos incorrectos	Mostrar mensaje de error indicando los datos inválidos
	Eliminar Personal	No se puede eliminar el empleado	Empleado tiene información asociada	Implementar eliminación segura con verificación de relaciones
			Error al eliminar información	Manejar correctamente las excepciones al

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

				eliminar
Gestionar Elementos del Paquete Elegido	Agregar Elemento	No se puede agregar el elemento	Error al validar datos o al agregar al paquete	Implementar validaciones correctas y verificar compatibilidad
			Servicio no existe	Verificar la existencia del servicio
	Eliminar Elemento	No se puede eliminar el elemento	Error al eliminar del paquete	Manejar correctamente las excepciones al eliminar
Gestionar Direcciones	Registrar Dirección	No se puede registrar la dirección	Error al validar datos o guardar información	Implementar validaciones correctas y manejo de excepciones
			Datos incompletos	Mostrar mensaje de error indicando los campos faltantes
	Editar Dirección	No se puede editar la dirección	Error al cargar la dirección o guardar cambios	Verificar existencia de la dirección y manejar excepciones
			Datos incorrectos	Mostrar mensaje de error indicando los datos inválidos
Visualizar Presentación de Paquetes	No se muestran los paquetes	Error al cargar información o mostrar presentación	Verificar disponibilidad de información y corregir errores en la presentación	
Buscar Servicios para Paquetes	No se encuentran resultados	Error en la búsqueda o no hay servicios disponibles	Implementar búsqueda eficiente y mostrar mensaje informativo si no hay resultados	
Gestionar Perfil	Editar Perfil	No se puede editar el perfil	Error al cargar la información o guardar cambios	Verificar existencia del usuario y manejar excepciones

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

			Datos incorrectos	Mostrar mensaje de error indicando los datos inválidos
Ver Eventos Pendientes	No se muestran los eventos	Error al cargar la información	Verificar disponibilidad de información y corregir errores en la presentación	
Marcar Eventos como Completados	No se puede marcar como completado	Error al actualizar el estado del evento	Manejar correctamente las excepciones al actualizar	
Acceso por Usuario y Contraseña	Autenticación fallida	Contraseña incorrecta o usuario no existe	Verificar la información de inicio de sesión	
			Ataque de fuerza bruta	Implementar mecanismos de defensa como captcha
Realizar Orden del Evento	No se puede realizar la orden	Error al validar datos o procesar pago	Implementar validaciones correctas y verificar integración con el procesador de pagos	
			Error al enviar correo electrónico	Implementar un sistema de reintentos y notificación de errores
Visualizar Servicios	No se muestran los servicios	Error al cargar la información	Verificar disponibilidad de información y corregir errores en la presentación	
Enviar Correo de Confirmación	No se envía el correo	Error al enviar correo electrónico	Implementar un sistema de reintentos y	

Proyecto	FS	Foodster
Cliente	DIPT	David Ivan Perez Torres

			notificación de errores	
Asignación de Trabajadores de Acuerdo a la Disponibilidad	No se asigna un trabajador	No hay trabajadores disponibles	Mostrar un mensaje informativo al usuario	
Calificar Paquetes/Servicios	No se puede calificar	Error al registrar la calificación	Manejar correctamente las excepciones al registrar la calificación	