

SISTEMA INFORMATICO DE GESTION DE ENTRENAMIENTO

Team Tryhard 3BC

Gestión de Proyecto Web

Segunda entrega

Docente

Nestor Piazza

Integrantes

Mathias Diaz

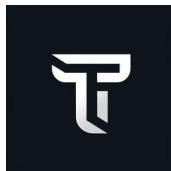
Alejo Tabares

Cristian Carpio

Brayan Rivero

Dylan Arrua

Montevideo 17 de Setiembre de 2024



Índice

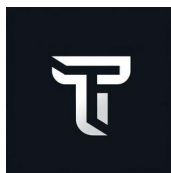
Índice	2
Introducción	3
Marco Teórico	4
Objetivos	8
Desarrollo	9
Diagrama Kanban (INICIAL)	9
Implementación de metodología Agile	10
Historias de usuario y criterios de aceptación de las mismas.	14
Ajuste de las métricas	20
Plan de contingencias	27
PROYECTO/SISTEMA	27
EMPRESA	30
Plan de riesgos	34
Gráficas de Esfuerzo	46
Actas de Reuniones (Segunda Entrega)	52
Anexo	57
Bibliografía	57



Introducción

Este documento aborda los aspectos fundamentales para la realización del proyecto web de egreso, siguiendo los lineamientos y requisitos establecidos por el docente de la asignatura Gestión de Proyectos.

A lo largo de esta documentación, se presentarán a detalle los procesos, análisis y conclusiones que salen del trabajo realizado por el equipo.



Marco Teórico

Metodología agile (Kanban y Scrum)

Las metodologías ágiles son una estrategia que impulsa a las organizaciones a gestionar los diferentes proyectos con rapidez y flexibilidad.

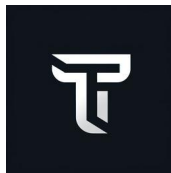
La metodología agile ayuda en el desarrollo de proyectos que necesitan más rapidez y mayor flexibilidad para adecuarse a lo que el cliente necesita. Siempre se enfoca en mejorar los resultados frente a proyectos realizados con metodologías tradicionales.

A diferencia de las formas tradicionales de gestionar los proyectos, las metodologías ágiles no necesitan definir al inicio de los proyectos la totalidad del alcance.

Los proyectos que son llevados a cabo con metodologías ágiles son capaces de adaptarse sobre la marcha, complementarse y resolverse en poco tiempo. Es decir, no se planifica ni se diseña el proyecto por adelantado, sino que a medida que se desarrolla se va definiendo el proyecto, gracias a un feedback constante.

Otra característica muy particular es que se trabaja por períodos de tiempo durante el cual cada miembro del equipo debe ejecutar una serie de tareas. Luego de ejecutar dichas tareas, se entregan los avances, se reciben devoluciones y comienza nuevamente el proceso, permitiendo implementar los cambios necesarios.

Existen diferentes metodologías ágiles, pero en este caso abordaremos Scrum y Kanban que aunque comparten principios ágiles, como la flexibilidad y la entrega continua de valor, se diferencian en su enfoque y estructura.



Scrum: Basada en ciclos de trabajo llamados **SPRINTS**, que suelen durar entre 1 y 4 semanas. En cada sprint, se planifica, desarrolla, revisa y se ajustan los entregables. Scrum incluye roles específicos (Product Owner, Scrum Master, y equipo de desarrollo) y eventos clave (reuniones diarias de 15 minutos, planificación del sprint, revisión y retrospectiva).

Kanban: Es un enfoque más flexible y fluido que utiliza un **TABLERO** visual para gestionar el flujo de trabajo. En Kanban, las tareas se representan como tarjetas y se mueven a través de diferentes columnas que reflejan su estado (por ejemplo, por hacer, en progreso, hecho). La idea es limitar la cantidad de trabajo en progreso para optimizar la eficiencia.

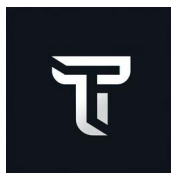
Historias de Usuario

Las historias de usuario son una herramienta utilizada en las metodologías de desarrollo ágiles para la especificación de los requisitos. Estas historias se redactan desde la perspectiva del usuario final, describiendo qué es lo que necesita, por qué lo necesita y qué valor aportará su implementación. Su principal objetivo es dividir el trabajo en unidades manejables, facilitando la comunicación entre los equipos de desarrollo y los clientes o usuarios.

Cada historia de usuario debe ser clara, concisa y fácilmente comprensible, y suele seguir el formato "Como (tipo de usuario), quiero (acción) para (beneficio/resultado)". Además, se complementan con criterios de aceptación que permiten verificar que los requisitos se han cumplido correctamente.

Cálculo de métricas del proyecto

Las métricas se utilizan para medir diferentes aspectos del proyecto, como el tamaño, la complejidad, el esfuerzo estimado y la calidad. Estas métricas proporcionan una base cuantitativa para la planificación y el seguimiento del proyecto. En esta entrega solo se realizaron ajustes.



Plan de contingencias

Un plan de contingencia es un conjunto de medidas y procedimientos diseñados para minimizar el impacto de imprevistos o crisis en una empresa. Un plan de contingencia brindará una alternativa para que la empresa pueda seguir adelante frente a diversas circunstancias imprevistas. Se trata de un plan de respaldo que reduce el estrés y minimiza los riesgos de fracaso que pueden afectar a todo proyecto.

Para elaborar un plan de contingencia se debe:

- Analizar riesgos y amenazas.
- Recopilar información esencial.
- Desarrollar una estrategia de respuesta.
- Elaborar un plan de respaldo.
- Revisar y actualizar el plan regularmente.
- Implementar y comunicar el plan.
- Evaluar el éxito.

Plan de riesgos

Un plan de gestión de riesgos es un documento en el que se definen los riesgos potenciales que pueden impedir el logro de objetivos en un proyecto, así como las acciones que es preciso implementar para neutralizar esas amenazas, disminuir su impacto negativo o aprovechar posibles oportunidades.

La redacción de un plan de gestión de riesgos es un trabajo de equipo. A veces, dependiendo del proyecto, este puede ser multidisciplinar, incluyendo personal de varias áreas relacionadas, como financiera, ingeniería, Alta Dirección o Gestión de Riesgos.

Proponemos una guía que se basa en siete pasos:

1. • Identificar los factores de Riesgo.



2. • Evaluar la probabilidad y el efecto sobre el proyecto.
3. • Desarrollo de estrategias para mitigar los riesgos.
4. • Monitorizar los factores de riesgo.
5. • Invocar el plan de contingencias.
6. • Gestionar la crisis.
7. • Recuperarse de la crisis.

Gráficas de Esfuerzo

Las gráficas de esfuerzo se refieren a herramientas visuales que ayudan a planificar, monitorear y gestionar la cantidad de esfuerzo o trabajo necesario para completar las tareas a lo largo del tiempo. Estas gráficas son fundamentales para garantizar que los recursos se utilicen de manera eficiente y que el proyecto se mantenga dentro de los plazos y el presupuesto planificados.



Objetivos

El proyecto como tal plantea la creación de un Sistema Informático de Gestión de Entrenamiento (S.I.G.EN). En esta materia específica, para la segunda entrega se plantea como objetivo principal la planeación estratégica de esta entrega utilizando metodologías ágiles, realizar correcciones de la anterior entrega y continuar con la planificación, control y monitoreo del desempeño del proyecto.

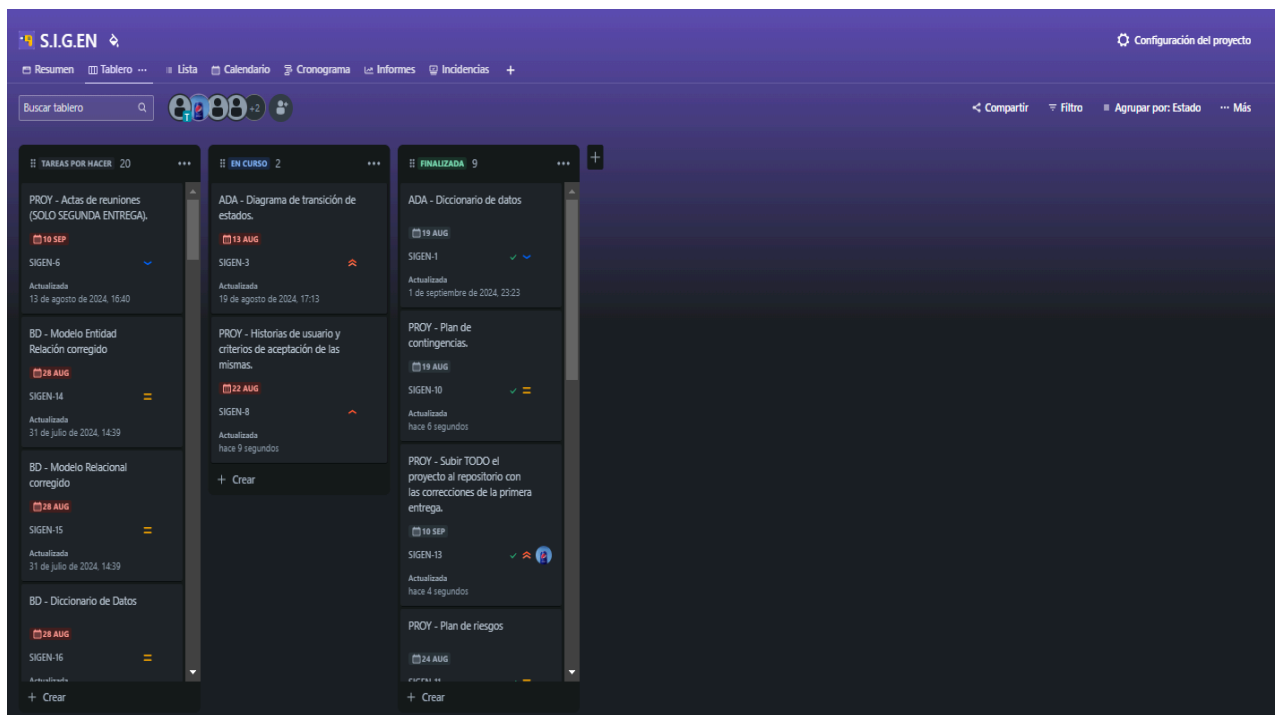
Para ello el docente, planteó diferentes objetivos, estos son:

- Diagrama Kanban e implementación.
- Actas de reuniones (SOLO SEGUNDA ENTREGA).
- Implementación de metodología Agile en coordinación con el Profesor de Análisis y Diseño de Aplicaciones (Propuesta y aplicación).
- Historias de usuario y criterios de aceptación de las mismas.
- Ajuste de las métricas. Plan de contingencias.
- Plan de riesgos
- Gráficas de esfuerzo.
- Subir TODO el proyecto al repositorio con las correcciones de la primera entrega.

Desarrollo

Diagrama Kanban (INICIAL)

Previo a la presentación del tema Metodología Agile por parte del docente, se comenzó trabajando con la implementación del Diagrama Kanban utilizando la herramienta JIRA. Esta herramienta sirvió en un primer momento para poder visualizar las diferentes tareas y asignarlas de manera ordenada con diferentes alertas para la realización de las mismas.





Implementación de metodología Agile

Posterior a la primera implementación del diagrama KANBAN y con conocimientos adquiridos sobre metodologías Agile, se comenzó su implementación utilizando la herramienta previamente mencionada, JIRA. En dicha herramienta se configuró un Proyecto de Software que integraba SCRUM y KANBAN en un solo lugar.

Conociendo la herramienta y estas dos metodologías, se procedió a cargar las diferentes tareas. Una vez ingresadas, se dividieron en tres sprints, cada uno con una duración de 8 días. El SCRUM MASTER, Mathias Díaz (Coordinador del grupo), fue el encargado de gestionar la carga de tareas y la creación de los sprints. En conjunto con el equipo de desarrollo, se realizó la asignación de tareas por sprint, evaluando tanto la dificultad de cada tarea como los conocimientos específicos de cada miembro del equipo.

Con esta estructura en, se continuó aplicando las metodologías, y el PRODUCT OWNER, Alejo Tabares (Sub-Coordinador del grupo), comenzó a jugar un papel relevante al encargarse de maximizar el valor del producto.

El link de acceso se encuentra en [Anexo](https://teamtryhard.atlassian.net/jira/software/projects/SGN/boards/3/backlog?atlassianOrigin=eyJpIjoiaNzUyMjZTBmYjFjNDQ4NGE3MTUzNDFiZTMwOWVmYzkiLCJwIjoiaaiJ9) o <https://teamtryhard.atlassian.net/jira/software/projects/SGN/boards/3/backlog?atlassianOrigin=eyJpIjoiaNzUyMjZTBmYjFjNDQ4NGE3MTUzNDFiZTMwOWVmYzkiLCJwIjoiaaiJ9>



A continuación se adjuntan imágenes de los diferentes sprints visualizados en el backlog y en el tablero KANBAN.

Sprint 1:

ID	Descripción	Fecha de vencimiento
SGM-1	ADA - Diccionario de datos	30 AUG
SGM-2	ADA - Diagrama de transición de estados	31 AUG
SGM-3	BD - Modelo Entidad Relación corregido	31 SEP
SGM-4	BD - Modelo Relacional corregido	31 SEP
SGM-5	BD - Diccionario de Datos	31 SEP
SGM-6	BD - Primera implementación de la Base de Datos en MySQL	31 SEP
SGM-7	PROY - Ajuste de las métricas	31 SEP
SGM-8	PROY - Gráficas de esfuerzo	31 SEP
SGM-9	PROY - Plan de riesgos	31 AUG
SGM-10	DW - HTML, CSS, JavaScript, PHP y Base de Datos	31 SEP
SGM-11	DW - Formularios	31 SEP
SGM-12	PROG - Login	31 AUG
SGM-13	PROG - Seguridad de SESSION	31 SEP
SGM-14	PROG - Código PHP	31 SEP
SGM-15	SO - Usuarios necesarios en el sistema operativo creados de acuerdo al estudio de roles	30 AUG
SGM-16	SO - Menú para el Operador del Centro de Cómputos (Administrador del Sistema), primera versión (contiene los scripts de usuarios, grupos, red, servicios, firewall y respaldo local)	30 AUG
SGM-17	SO - Configuraciones de red en las terminales y el servidor	30 AUG
SGM-18	FEMP - Plan de Inversiones	31 AUG
SGM-19	PROY - Plan de contingencias	31 SEP

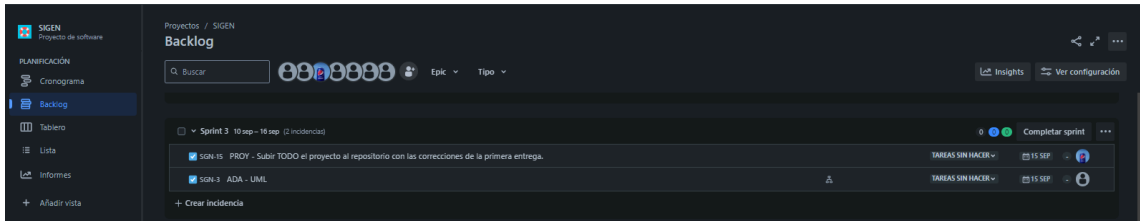
Kanban Sprint 1

TAREAS SIN HACER	TAREAS EN PROCESO	TAREAS HECHAS 19 DE 29
+ Crear incidencia		ADA - Diccionario de datos SPRINT 1 30 AUG ✓
		ADA - Diagrama de transición de estados SPRINT 1 31 AUG ✓
		BD - Modelo Entidad Relación corregido SPRINT 1 31 SEP ✓
		BD - Modelo Relacional corregido SPRINT 1 31 SEP ✓
		BD - Diccionario de Datos SPRINT 1 31 SEP ✓
		BD - Primera implementación de la Base de Datos en MySQL SPRINT 1 31 SEP ✓

The screenshot displays the Sigen project management tool. On the left, a sidebar contains navigation options: PLANIFICACIÓN (with sub-items Cronograma, Backlog, Tablero, Lista, Informes), DESARROLLO (with sub-item Código), and other project-related links. The main area shows a Kanban board for 'Sprint 2'. At the top, there's a search bar and a filter dropdown set to 'Sprint 2'. Below this, tasks are organized into columns: 'TAREAS SIN HACER' (containing one task '+ Crear incidencia'), 'TAREAS EN PROCESO' (empty), and a third column (containing several tasks). A dropdown menu is open over the 'Sprint 2' filter, showing a list of sprints. The tasks listed include 'SGN-38', 'PROG - Datos de prueba', 'PROG - Manejo de entidades', 'DW - JavaScript', 'BD - Sentencias SQL', and 'BD - Diagrama de Bachman', each with associated icons for status, priority, and assignment.

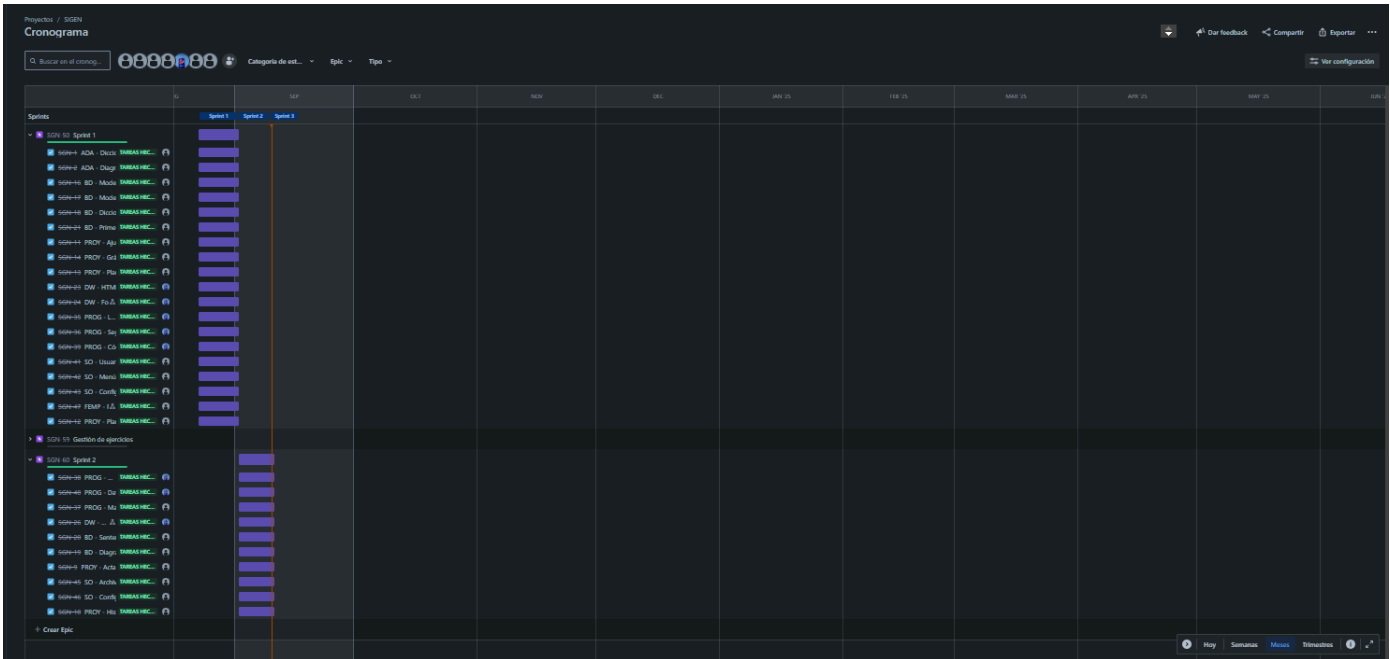


Sprint 3 Backlog



KANBAN SPRINT 3

Agregado a esto tenemos la pestaña cronograma donde podemos visualizar las diferentes tareas separadas por sprint en una especie de GANTT.





Historias de usuario y criterios de aceptación de las mismas.

Una vez realizada la implementación de las metodologías agile continuamos con la creación de las historias de usuarios (USER STORIES), las mismas se pueden ver en el backlog del [JIRA](#). Además, acá, se adjuntan las historias con los diferentes criterios de aceptación.

HISTORIA DE USUARIO - 1	Dificultad
Administrador Registra Clientes	3
COMO Administrador QUIERO registrar clientes y entrenadores a través de un formulario PARA registrar sus datos en el sistema y que accedan al mismo.	
<u>Criterios de aceptación</u>	Riesgo
Dado que quiero registrar clientes y entrenadores en el sistema Cuando en el formulario ingrese los datos de los mismos Entonces el sistema deberá permitir el registro de los mismos y mostrar un mensaje de éxito.	2



HISTORIA DE USUARIO - 2	Dificultad
Cliente se registra en el sistema	2
Como cliente quiero registrarme en el sistema a través de un formulario para poder acceder a todas las funcionalidades del sistema.	
<u>Criterios de aceptación</u>	Riesgo
Dado que quiero registrarme en el sistema Cuando en el formulario ingrese los datos pertinentes Entonces el sistema deberá aceptar el registro y mostrar un mensaje de éxito para luego permitirme el acceso al mismo.	1

HISTORIA DE USUARIO - 3	Dificultad
Creación de ejercicios	5
Como entrenador quiero poder crear ejercicios en el sistema a través de un formulario para poder ofrecer rutinas específicas a los clientes.	



<u>Criterios de aceptación</u>	Riesgo
<p>Dado que quiero crear ejercicios en el sistema,</p> <p>Cuando rellene el formulario de creación de los mismos,</p> <p>Entonces el sistema deberá crear el ejercicio y mostrar un mensaje de éxito confirmando la acción.</p>	3

HISTORIA DE USUARIO - 4	Dificultad
Modificación de ejercicios	3
Como entrenador quiero modificar ejercicios en el sistema a través de un formulario para poder ofrecer nuevas rutinas a los clientes.	
<u>Criterios de aceptación</u>	Riesgo
<p>Dado que quiero modificar ejercicios en el sistema,</p> <p>Cuando rellene el formulario de modificación de los mismos,</p>	2



Entonces el sistema deberá modificar el ejercicio y mostrar un mensaje de éxito confirmando la acción.

HISTORIA DE USUARIO - 5	Dificultad
Eliminación de ejercicios	2
Como entrenador quiero eliminar ejercicios en el sistema a través de un botón para poder eliminar los ejercicios existentes.	
<u>Criterios de aceptación</u>	Riesgo
<p>Dado que quiero eliminar ejercicios en el sistema,</p> <p>Cuando apreté el botón de eliminación de los mismos, y además confirme la acción</p> <p>Entonces el sistema deberá eliminar el ejercicio.</p>	1



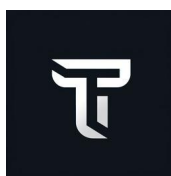
HISTORIA DE USUARIO - 6	Dificultad
Asignación de ejercicios a combos	8
Como entrenador quiero asignar ejercicios a un combo para poder personalizar las rutinas de los clientes.	
<u>Criterios de aceptación</u>	Riesgo
<p>Dado que quiero asignar asignar ejercicios a un combo específico,</p> <p>Cuando rellene el formulario de combos de ejercicios</p> <p>Entonces el sistema creará el combo para poder personalizar la rutina de los clientes.</p>	5

HISTORIA DE USUARIO - 7	Dificultad
Creación de deportes	3
Como Administrador quiero agregar deportes en el sistema para poder tener una mejor oferta para los clientes.	



<u>Criterios de aceptación</u>	Riesgo
<p>Dado que quiero agregar deportes en el sistema,</p> <p>Cuando rellene el formulario de creación de deportes y confirme la acción</p> <p>Entonces el sistema deberá crear el deporte.</p>	2

HISTORIA DE USUARIO - 8	Dificultad
Creación de deportes	5
<p>Como Cliente quiero visualizar mi plan de entrenamiento asignado por el entrenador para poder realizar mi rutina de ejercicios.</p>	
<u>Criterios de aceptación</u>	Riesgo
<p>Dado que quiero visualizar mi plan de entrenamientos en el sistema,</p> <p>Cuando esté en la sección de rutinas</p> <p>Entonces el sistema desplegará la rutina que tengo asignada.</p>	3



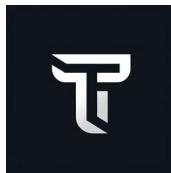
Ajuste de las métricas

En base a lo ya avanzado, se mejoró las métricas por puntos de función que fueron realizadas para la primer entrega, se corrigieron datos de entradas para tener los puntos exactos, los resultados:

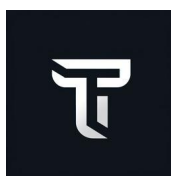
COMPUTACIÓN DE MÉTRICAS DE PUNTO DE FUNCIONES.						
	Factor de ponderación.					
Parámetro de medición	Cuenta	Simple	Medio	Complejo		Total
Número de entradas de usuario	23	3	4	6	=	69
Número de salidas de usuario	12	4	5	7	=	48
Número de peticiones de usuario	8	3	4	6	=	24
Número de archivos	3	7	10	15	=	21
Número de interfaces externas	1	5	7	10	=	5
Cuenta = Total						167
Nº de entradas de usuario	Los datos ingresados por el usuario.					
Nº de salidas de usuario	Informes, pantallas, mensajes de error .					
Nº de peticiones de usuario	Entradas interactivas					
Nº de archivos	Archivos maestro (lógico)					
Nº de interfaces externas	Todos los dispositivos que se utilicen para intercambiar datos.					

PF.= Cuenta-Total * (0,65+0,001* sumatoria de Fi)						
Fi (i=1 a 14) son los valores de ajuste de complejidad.						
AJUSTE DE COMPLEJIDAD						
	0	1	2	3	4	5
	No influencia	Incident al	Modera do	Medio	Signific ativo	Esencia l
1. ¿Requiere el sistema copias de seguridad y recup. fiables?						SI
2. ¿Se requiere comunicac. de datos ?						SI
3.¿ Existen funciones de func. distribuido?				SI		
4. ¿ Es crítico el rendimiento?					SI	
5. ¿ Se ejecutará el sistema en un entorno operativo existente y fuertemente utilizado ?					SI	
6- ¿ Requiere el sistema entrada de datos interactiva ?						SI
7. ¿ Requiere la entrada de datos interactivas que las transac. de entrada se lleven a cabo sobre					SI	

múltiples pantallas u operaciones ?						
8. ¿ Se actualizan los archivos maestro en forma interactiva ?					SI	
9. ¿ Son complejas las entradas, las salidas, los archivos o las peticiones?		SI				
10. ¿ Es complejo el procesamiento interno ?				SI		
11. ¿ Se diseñará el código para ser reutilizable ?						SI
12. ¿ Están incluidas en el diseño la conversión y la instalación ?						SI
13. ¿ Se diseñará el sistema para múltiples instalaciones en diferentes organizaciones ?	SI					
14. ¿ Se diseñará la aplicación para facilitar los cambios y para ser fácilmente utilizada por el usuario ?						SI
	0	1	0	6	16	30
			Fi =	53		



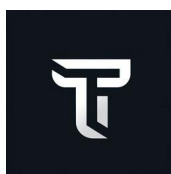
PF.= Cuenta-Total * (0,65+0,001* sumatoria de Fi)		=	117			
TAMAÑO DEL PROYECTO y COSTOS DEL PROYECTO.						
Lenguaje DE PROGRAMACIÓN		LDC/PF	TOTAL S			
Ensamblador		320	37568.3 2			
C		128	15027.3 28			
COBOL		105	12327.1 05			
FORTRAN		105	12327.1 05			
PASCAL		90	10566.0 9			
ADA		70	8218.07			
LENGUAJES ORIENTADO A OBJET.		30	3522.03			
LENGUAJES DE 4a.GENERACION		20	2348.02			
GENERADORES DE CÓDIGO		15	1761.01 5			
HOJAS DE CÁLCULO		6	704.406			
LENGUAJES GRÁFICOS (ICONOS)		4	469.604			
VALOR ESPERADO = (OPTIM +4PROBABLE+PESIMISTA)/6						
VALOR ESPERADO =	3071.9928 33	lineas				



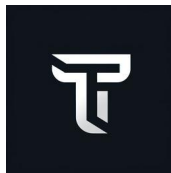
Según valores tomados de la bibliografía específica , se describen 620 Líneas/mes						
	tiempo total =	4.95				
		15855.4				
	Costos=	4688 dólares				
Se consideró un salario de U\$S	20	por hora				
Trabajando	160	horas por mes				

Para ajustar todo se decidió desglosar todo de la siguiente manera.

Nº de entradas de usuario	Los datos ingresados por el usuario.
1	Ingresar Nombre
2	Ingresar Apellido
3	Ingresar Email
4	Ingresar Documento de identidad
5	Ingresar Peso
6	Ingresar Estatura
7	Ingresar Numero Telefonico
8	Ingresar Contraseña
9	Ingresar Contraseña Nuevamente
10	Ingresar Numeros de la tarjeta Frontales
11	Ingresar Fecha de Vencimiento de la tarjeta
12	Ingresar Numeros de la tarjeta Reverso o CCV
13	Ingresar Nombre del Gimnasio
14	Ingresar Direccion Del Gimnasio
15	Ingresar Instagram Del Gimnasio
16	Ingresar Nombre del Plan De Ejercicio
17	Ingresar Duracion del plan de Ejercicio
18	Ingresar descripción del plan de Ejercicio
19	Ingresar Nombre Del Ejercicio
20	Ingresar Musculo Que Trabaja El Ejercicio



21	Ingresar descripción Del Ejercicio
22	Ingresar Nombre Del Combo De Ejercicios
23	Ingresar descripción Del Combo De Ejercicios
Nº de salidas de usuario	Informes, pantallas, mensajes de error .
1	Error Usuario o Contraseña incorrectos Intente Nuevamente
2	Error al completar El Pago Su tarjeta ha expirado, Saldo insuficiente
3	Felicidades Su Registro se ha completado Correctamente
4	Gracias Su pago ha sido Procesado Correctamente
5	Felicidades Usted Ha sido Agendado Satisfactoriamente
6	Muchas Gracias Por Su Reporte
7	Error Al Cambiar Contraseña Su contraseña (No Puede Ser Igual A la Contraseña Actual)
8	Cambio De Contraseña Realizado Correctamente Intente Ingresar a su cuenta
9	Cambio De Contraseña Realizado Correctamente Intente Ingresar a su cuenta
10	Felicidades el combo de ejercicios ha quedado registrado exitosamente
11	Felicidades el plan de ejercicio ha quedado registrado correctamente
12	Felicidades el gimnasio ha quedado creado correctamente
Nº de peticiones de usuario	Entradas interactivas
1	Seleccione Idioma
2	Subir Logo
3	Seleccione Tipo De Documento
4	Ingresar Fecha De Nacimiento
5	Subir Imagen de Ejercicio
6	Lista De Ejercicios
7	Ingresar Forma De Pago



Nº de archivos	Archivos maestro (lógico)				
1	Archivo de Clientes				
2	Archivo de Cuentas de Usuario				
3	Archivo de Empleados				



Plan de contingencias

Se realizó el plan de contingencias del proyecto y el de la empresa, estos son:

PROYECTO/SISTEMA

Identificación de Riesgos

Fallas técnicas del software:

- Bugs críticos que afecten la funcionalidad básica del gestor.
- Caída del sistema o pérdida de datos.

Problemas de integración:

- Incompatibilidad con dispositivos o sistemas operativos específicos.
- Dificultad para integrar el software con otros sistemas del gimnasio.

Retrasos en el desarrollo:

- Problemas en la planificación o ejecución del proyecto.
- Ausencia o baja productividad del equipo por enfermedad, vacaciones, renuncias o alguna otra particularidad.

Problemas de seguridad:

- Vulnerabilidades que puedan ser explotadas para robar datos sensibles de los clientes o del gimnasio.
- Falta de cumplimiento con normativas de protección de datos.

Problemas financieros:

- Sobrecostos inesperados.
- Reducción del presupuesto por decisiones administrativas.

Problemas con los proveedores:



- Retrasos en la entrega de herramientas o recursos necesarios para el desarrollo.
- Mal funcionamiento de software o servicios de terceros.

Resistencia al cambio:

- Los usuarios finales (entrenadores y fisioterapeutas) no logran adaptarse al uso del nuevo sistema.
- Necesidad de formación adicional que no fue considerada inicialmente.

Estrategias de Contingencia

Fallas técnicas del software

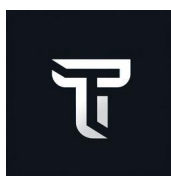
- Implementar un plan de pruebas exhaustivo para detectar y corregir bugs antes de la implementación. Contar con un equipo de soporte técnico disponible 24/7 para resolver problemáticas críticas. Recursos necesarios: equipo de QA, herramientas de monitoreo, personal de soporte técnico. Responsables: Líder del equipo de desarrollo y líder de soporte técnico.

Problemas de integración

- Realizar pruebas de integración tempranas y continuas con los sistemas existentes del gimnasio (si existen). Establecer un canal de comunicación con los proveedores de los sistemas a integrar. Recursos necesarios: equipo de desarrollo, documentación de APIs y sistemas existentes, contacto con proveedores. Responsables: Líder de desarrollo y encargado del proceso de integración.

Retrasos en el desarrollo

- Revisar el cronograma del proyecto regularmente y ajustar las prioridades según sea necesario. Implementar metodologías ágiles para



mayor flexibilidad. Recursos necesarios: herramientas de gestión de proyectos, reuniones regulares de seguimiento, metodologías ágiles. Responsables: Project Manager y Scrum Master.

Problemas de seguridad

- Realizar auditorías de seguridad periódicas, aplicar actualizaciones y utilizar prácticas de desarrollo seguro como codificación segura y pruebas de penetración. Recursos necesarios: herramientas de seguridad, equipo de seguridad informática, políticas de privacidad y protección de datos. Responsables: Líder de seguridad y equipo de desarrollo.

Problemas financieros

- Mantener una reserva financiera para imprevistos, realizar revisiones presupuestarias periódicas y ajustar los gastos según las necesidades del proyecto. Recursos necesarios: reserva financiera, herramientas de gestión financiera, revisión de contratos. Responsables: CFO y Project Manager.

Problemas con los proveedores

- Establecer acuerdos de nivel de servicio (SLAs) claros con los proveedores y tener alternativas en caso de fallas críticas. Recursos necesarios: contratos con proveedores, lista de proveedores alternativos, equipo de adquisiciones. Responsables: Encargado de adquisiciones y Project Manager.

Resistencia al cambio

- Realizar sesiones de capacitación y talleres para entrenadores y fisioterapeutas, e incluir a los usuarios finales en las fases de diseño y pruebas para asegurar la usabilidad. Recursos necesarios: materiales de capacitación, instructores, sesiones de feedback. Responsables: Líder de implementación y encargado de formación.



Plan de Comunicación

- El objetivo del plan de comunicación es mantener a todas las partes interesadas informadas sobre el progreso del proyecto y cualquier problema que surja. Recursos necesarios: reuniones semanales con el equipo de desarrollo, informes quincenales para la dirección del gimnasio, reuniones mensuales con los usuarios finales. Medios: correos electrónicos, plataformas de gestión de proyectos, videoconferencias. Responsable: Project Manager.

Revisión y Mejora Continua

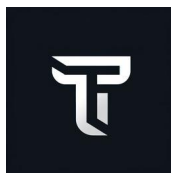
- Para que el plan de contingencia sea efectivo, se recomienda realizar una revisión trimestral para mantener actualizada la información. Responsables: Project Manager y equipo de liderazgo. Metodologías: análisis de riesgos y revisión de incidentes pasados para mejorar el plan.

EMPRESA

Evaluación de Riesgos:

Se identifican los riesgos potenciales que podrían afectar la operatividad de la empresa. Algunos ejemplos son los siguientes:

- Fallas en el servidor: Pérdida de acceso a los servidores donde se alojan las aplicaciones.
- Ciberataques: Hackers, malware, phishing que pueden comprometer la seguridad de los datos.
- Problemas de conectividad: Caída del servicio de internet o problemas con los proveedores de servicios de red.
- Errores humanos: Despliegues fallidos, eliminación accidental de datos, etc.

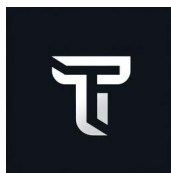


- Desastres naturales: Inundaciones, terremotos, incendios que afecten las instalaciones físicas.
- Fallas en el suministro eléctrico: Corte de electricidad prolongado que impida el funcionamiento de los servidores y estaciones de trabajo.
- Problemas legales o de incumplimiento: Brechas en el cumplimiento de normativas de Protección de datos.
- Incumplimiento en tiempos: No cumplir con los tiempos estipulados de las entregas.
- Mala administración del personal: No repartir equitativamente el trabajo necesario para cumplir con el objetivo en común.

Estrategias de Mitigación:

Definir ciertas estrategias para mitigar los riesgos identificados:

- Respaldo de Datos: Implementar políticas de respaldo periódico de datos en múltiples ubicaciones geográficas, como servidores propios o la nube.
- Seguridad Cibernética: Adoptar medidas de seguridad robustas, como firewalls, autenticación multifactor, cifrado de datos y auditorías regulares de seguridad.
- Plan de Recuperación de Desastres: Desarrollar un plan para la restauración rápida de servicios en caso de un desastre, incluyendo servidores redundantes y planes de contingencia para el personal.
- Capacitación del Personal: Capacitar a los empleados en mejores prácticas de seguridad y en la respuesta a emergencias.
- Redundancia en Conectividad: Contratar múltiples proveedores de servicios de internet para evitar caídas por problemas con uno solo.
- Generadores de Energía: Tener generadores de emergencia en caso de fallos en el suministro eléctrico.
- Comunicación: El referente de grupo debe hacer énfasis en que sus indicaciones de trabajo sean comprendidas correctamente por el equipo.



Además, asegurar que haya una comunicación clara entre los miembros del equipo.

- Documentación Legal y de Cumplimiento: Mantener al día la documentación legal y garantizar que todas las aplicaciones cumplan con las normativas relevantes.
- Gerencia general: Hacer reuniones periódicas donde se anuncien novedades, problemáticas, y servir de foro para buscar soluciones a los conflictos del momento.

Plan de Comunicación:

Establecer un plan de comunicación para informar a todas las partes interesadas en caso de ser necesaria una contingencia:

- Clientes: Informar rápidamente a los clientes sobre cualquier interrupción del servicio, las causas y los pasos que se están tomando para resolver el problema.
- Empleados: Definir canales de comunicación claros para que los empleados sepan cómo actuar y a quién reportar en caso de ser necesaria una contingencia.
- Proveedores: Coordinar con proveedores claves para garantizar la continuidad del suministro de servicios esenciales.

Plan de Respuesta y Recuperación:

Detallar las acciones específicas a seguir en caso de que sea necesaria alguna contingencia:

- Ante la falla en servidores:
 - Activar servidores de respaldo.
 - Notificar al equipo de TI y a los proveedores de hosting.
 - Comunicar a los clientes y mantenerlos actualizados.
- Ante un ciberataque:
 - Desconectar los sistemas comprometidos de la red.
 - Activar los protocolos de respuesta ante incidentes de seguridad.



- Informar a las autoridades si es necesario.
 - Iniciar una investigación para determinar el alcance del ataque.
- Ante problemas de conectividad:
 - Conmutar a un proveedor de servicios de internet alternativo.
 - Notificar a los empleados y clientes si el problema persiste.
- Ante algún desastre natural:
 - Garantizar la seguridad del personal.
 - Activar el plan de recuperación de desastres.
 - Comunicarse con los clientes y empleados sobre la situación.
- Ante una mala gestión:
 - Llamar a junta urgente.
 - Debatir sobre los errores cometidos.
 - Llegar a una solución en conjunto.

Pruebas y Simulacros:

Realizar simulacros regulares para probar la efectividad del plan de contingencia. Asegurarse de que todos los empleados conozcan su rol en caso de emergencia y que el plan sea revisado y actualizado regularmente.

Revisión del Plan y Mejora Continua:

Después de cualquier incidente o simulacro, se deberá revisar qué tan efectivo fue el plan y hacer ajustes si es necesario. La retroalimentación constante es clave para mejorar la resiliencia de la empresa.



Plan de riesgos

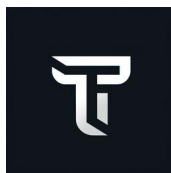
Posterior a la realización de los planes de contingencias se realizó el plan de riesgos:

1. Identificación de los factores de Riesgo.

Para comenzar con el plan de gestión de riesgos, se comenzó realizando un análisis de la situación actual del cliente. La información que se recabo para la Especificación de Requerimientos es que el cliente no cuenta con un sistema actualmente, solamente utiliza planillas electrónicas.

Teniendo el análisis se comenzó con la identificación de los diferentes factores de riesgos, ellos son,

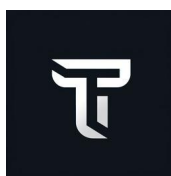
- Resistencia al cambio
 - El uso de un nuevo sistema puede generar problemas por posibles descontentos de los usuarios finales del software.
 - Es posible que se necesite capacitación para que el personal pueda utilizar el sistema de manera efectiva.
- Migración de datos
 - Al migrar los datos que el cliente tiene almacenados en las planillas de excel al software se corren riesgos de pérdida de los mismos.
- Adaptabilidad y Escalabilidad
 - El software deberá funcionar en el hardware presentado por el cliente, para ello se debe pensar en la limitación de ciertas funcionalidades que puedan exceder los tiempos de espera.
 - El software debe ser robusto y permitir una gran cantidad de usuarios conectados de manera simultánea.
- Seguridad de la información
 - El sistema manejaría información sensible de los usuarios. Un fallo en la seguridad podría llevar a filtraciones de información



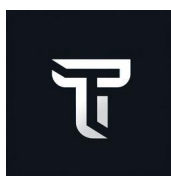
- Ciberseguridad: Existe el riesgo de ataques cibernéticos, como hackeos, ransomware, o ataques DDoS, que podrían comprometer la integridad del sistema.
- Mantenimiento del sistema
 - El software requiere actualizaciones continuas y mantenimiento para asegurar su funcionamiento adecuado y seguro. No realizar esto adecuadamente puede llevar a vulnerabilidades o desactualización del sistema.
- Competencia
 - Se debe tener en cuenta a los diferentes competidores dentro del mercado que puedan ofrecer los mismos productos.

2. Evaluación de la probabilidad y el efecto sobre el proyecto/sistema

- Riesgo: **Resistencia al cambio**
 - Probabilidad: Alta
 - Dado la falta de costumbre de los usuarios finales a utilizar el software, la probabilidad de la resistencia al cambio es alta
 - Impacto: Medio
 - El impacto es medio por la falta de conocimiento de los usuarios finales
- Riesgo: **Migración de datos**
 - Probabilidad: Media
 - Existe una probabilidad de perder datos en la migración de los mismos por el mecanismo antiguo utilizado por el cliente para el almacenamiento de los mismos.
 - Impacto: Alta
 - La pérdida de estos datos sería de un gran impacto porque se estarían perdiendo datos muy valiosos para la empresa.
- Riesgo: **Adaptabilidad y Escalabilidad**



- Probabilidad: Media
 - Existe la posibilidad que el software no funcione de manera óptima en el hardware del cliente si el mismo tiene limitaciones.
- Impacto: Alto
 - Un software que no se adapte al hardware o que no sea escalable podría causar tiempos de espera muy largos, por ende los usuarios no estarían satisfechos con el mismo.
- Riesgo: **Seguridad de la información**
 - Probabilidad: Media
 - Siempre existe la posibilidad que el software sufra algún problema relacionado a la seguridad, sea estos problemas por errores humanos o ataques DDoS.
 - Impacto: Alto
 - Un fallo en la seguridad estaría permitiendo la filtración de datos importantes y sensibles, también generaría desconfianza por parte de los usuarios, además de problemas legales.
- Riesgo: **Mantenimiento del sistema**
 - Probabilidad: Alta
 - Es necesario mantener el software actualizado para evitar fallos y vulnerabilidades.
 - Impacto: Alto
 - La falta de mantenimiento provocaría fallos en el sistema y exposición a amenazas de seguridad poniendo en riesgo datos de los usuarios.
- Riesgo: **Competencia**
 - Probabilidad: Alta
 - Existen muchas empresas que ofrecen productos similares, y los clientes podrían optar por la competencia si no se ofrece un producto innovador o con mejor soporte.



- Impacto: Medio
 - Un buen producto con un soporte adecuado puede mitigar el impacto de la desviación de clientes hacia la competencia, pero aún así, el riesgo sigue presente.

3. Desarrollo de estrategias para mitigar los riesgos.

Para mitigar los riesgos identificados, se pueden implementar dos tipos de estrategias: Plan de Acción, para minimizar o eliminar el riesgo, y Plan de Contingencia, para aceptar el riesgo y tener un plan en caso de que el problema se materialice.

Estrategias por riesgo:

- Resistencia al cambio
 - Plan de Acción: capacitación a los usuarios finales, involucrándolos en fases de diseño y pruebas.
 - Plan de Contingencia: proveer soporte post-implementación para resolver dudas o problemas de adaptación.
- Migración de datos
 - Plan de Acción: realizar pruebas y copias de seguridad de los datos antes de la migración.
 - Plan de Contingencia: establecer un plan de restauración de datos en caso de pérdida.
- Adaptabilidad y escalabilidad
 - Plan de Acción: optimizar el software para que funcione en hardware de bajo rendimiento y realizar pruebas de carga.
 - Plan de contingencia: limitar el número de funcionalidades si se detectan problemas de rendimiento.
- Seguridad de la información
 - Plan de Acción: implementar buenas prácticas de ciberseguridad, como encriptación de datos y autenticación robusta.



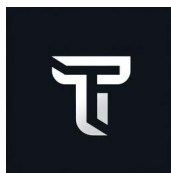
- Plan de Contingencia: desarrollar un plan de respuesta ante incidentes de seguridad.
- Mantenimiento del sistema
 - Plan de Acción: establecer un cronograma de mantenimiento y actualizaciones periódicas.
 - Plan de Contingencia: tener personal capacitado en soporte técnico y un sistema de alertas para detectar problemas.
- Competencia
 - Plan de Acción: innovar y mejorar continuamente el software, además de ofrecer soporte técnico eficiente.
 - Plan de Contingencia: monitorear las ofertas de los competidores y ajustar precios o características del producto si es necesario.



4. Monitorizar los factores de riesgo

Definir Indicadores Clave de Riesgo (KRI):

- Resistencia al cambio:
 - Indicadores: Número de problemas reportados por los usuarios finales, solicitudes de soporte y participación en las posibles capacitaciones.
 - Medida: Encuestas a los usuarios finales para comprobar la adaptación.
- Migración de datos:
 - Indicadores: Pérdida o corrupción de datos durante la migración, porcentaje de datos migrados exitosamente.
 - Medida: Pruebas de migración.
- Adaptabilidad y escalabilidad:
 - Indicadores: Tiempo de respuesta del sistema, cantidad de usuarios simultáneos.
 - Medida: Pruebas de carga y rendimiento.
- Seguridad de la información:
 - Indicadores: Número de intentos de acceso no autorizado, alertas de seguridad.
 - Medida: Auditorías de seguridad, monitoreo en tiempo real de la actividad en el sistema.
- Mantenimiento del sistema:
 - Indicadores: Número de fallos reportados, cumplimiento del cronograma de mantenimiento (2 anuales según E.S.RE).
 - Medida: Registros de mantenimiento, informes de actualizaciones.
- Competencia:



- Indicadores: Análisis de mercado (realizado en Formación Empresarial), desviación de clientes hacia la competencia.
- Medida: Comparativa de ofertas de la competencia, tasa de retención de clientes.

Trazabilidad: Cada factor de riesgo debe ser medido mediante métricas.

Límites de Control: Para cada indicador de riesgo, se deben definir límites de control (por ejemplo, un umbral de aceptación para los tiempos de respuesta o una cantidad máxima de errores en la migración de datos).

Revisión y Actualización Continua: Los riesgos pueden evolucionar a medida que el proyecto avanza. Se deben hacer revisiones continuas para reevaluar los riesgos y readaptar la mitigación de los mismos.

5. Invocar el plan de contingencias.

1- Detección del Exceso de Límites de Control

Cuando un indicador clave de riesgo sobrepasa el límite de control establecido (por ejemplo, si un bug crítico interrumpe el funcionamiento básico del software o si hay una caída del sistema), se deben tomar medidas inmediatas según el nivel del exceso.

2- Notificar el problema a nivel operativo

Posterior a la detección del problema, se debe notificar a los responsables de solucionarlo, en nuestro caso el grupo entero.

3- Activación del plan de contingencia

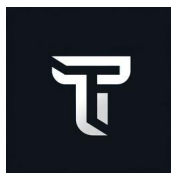
Si, tras las primeras acciones correctivas, el problema no se corrige y se excede el siguiente límite de control, se deberá activar el plan de contingencia



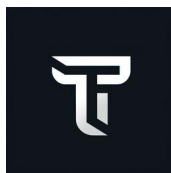
previsto. Este plan incluye medidas previamente definidas para mitigar el impacto del riesgo.

Ejemplos de Activación del Plan de Contingencia según Riesgo:

- **Fallas técnicas del software:**
 - Escenario: Se detecta un bug crítico que afecta la funcionalidad básica del software.
 - Acciones operativas: El equipo de desarrollo intenta resolver el bug con un parche urgente. Si no se resuelve dentro del tiempo límite operativo (por ejemplo, 4 horas), el problema escalará.
 - Activación del Plan de Contingencia:
 - Se realiza un rollback a una versión anterior del software.
 - El equipo trabaja para solucionar el bug crítico de manera urgente.
 - Se implementan herramientas de monitoreo para identificar y corregir otros posibles bugs antes de que causen mayores interrupciones.
 - En caso de pérdida de datos, se activa el plan de restauración desde las copias de seguridad más recientes.
- **Problemas de integración:**
 - Escenario: El software es incompatible con uno de los sistemas o dispositivos clave del cliente, afectando la operatividad.
 - Acciones operativas: Se intentan solucionar las incompatibilidades mediante ajustes en la configuración del software y en los dispositivos del cliente.
 - Activación del Plan de Contingencia:
 - El equipo de desarrollo trabaja en un parche específico para solucionar la incompatibilidad.
 - Se coordina con los proveedores de los dispositivos o sistemas incompatibles para obtener documentación técnica y realizar los ajustes necesarios.



- En caso de que el problema persista, se considera la opción de una solución temporal hasta que la integración sea resuelta.
- Problemas de seguridad:
 - Escenario: El sistema es vulnerable a un ataque cibernético (DDoS, ransomware, hackeo) que podría comprometer la información sensible.
 - Acciones operativas: Se implementan medidas inmediatas para reforzar la seguridad, como bloquear accesos no autorizados y aplicar parches de emergencia.
 - Activación del Plan de Contingencia:
 - El equipo activa el plan de respuesta a problemas y toma medidas para aislar la parte comprometida del sistema.
 - Se notifica a las partes afectadas (clientes y usuarios) sobre el incidente.
 - Se inician procesos para identificar las vulnerabilidades explotadas y se aplican soluciones permanentes.
 - En caso de pérdida de datos sensibles, se activan protocolos de restauración de copias de seguridad y se aplican medidas de protección de datos.
- Resistencia al cambio:
 - Escenario: Los usuarios finales del sistema (entrenadores, fisioterapeutas) muestran resistencia al uso del nuevo software y se reportan constantes problemas o quejas sobre su funcionalidad.
 - Acciones operativas: Se realizan sesiones de capacitación adicionales para abordar las preocupaciones inmediatas de los usuarios.
 - Activación del Plan de Contingencia:



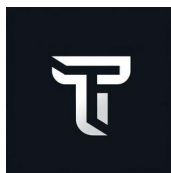
- Se organiza un programa de formación que incluye guías paso a paso, demostraciones en vivo y tutoriales personalizados.
- Se implementa un equipo dedicado para asistir a los usuarios durante el proceso de adaptación.
- Se toma en cuenta el feedback de los usuarios para realizar ajustes en la interfaz del software o agregar funcionalidades que faciliten su uso.

6. Gestionar la Crisis

Una vez activado el plan de contingencia, la gestión de la crisis implica una supervisión constante y rápida adaptación. El hecho de haber anticipado la crisis no significa que el equipo puede relajarse; más bien, es necesario mantenerse alerta y monitorear tanto la evolución de la crisis como otros aspectos del proyecto que puedan verse afectados indirectamente.

Estrategias para Gestionar la Crisis:

- Monitoreo constante:
 - Es crucial seguir de cerca el impacto del plan de contingencia y verificar si está funcionando como se había previsto.
- Evaluar la efectividad del plan de contingencia:
 - Si el plan de contingencia está funcionando adecuadamente, se debe continuar con la ejecución y seguir ajustando los detalles operativos necesarios.
 - Si el plan fracasa (por ejemplo, no se logra detener la pérdida de datos o el rendimiento sigue deteriorándose), se debe declarar una situación de crisis.
- Escalar decisiones:
 - En una situación de crisis más severa (como la caída completa del sistema), se deberá escalar el problema a los líderes del proyecto y tomar decisiones más drásticas, como cambiar de



estrategia de mitigación, aplicar medidas extremas o detener temporalmente el proyecto para evitar mayores daños.

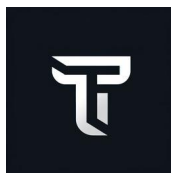
- Comunicación efectiva:
 - Durante la crisis, es esencial mantener una comunicación fluida con todas las partes interesadas. Esto incluye informar sobre el progreso de las medidas de contingencia y las decisiones que se están tomando en tiempo real.
 - Utilizar herramientas de comunicación para notificar al equipo sobre cambios en prioridades o necesidades de recursos.
- Documentar la crisis:
 - Toda la información y las acciones tomadas durante la crisis deben ser documentadas de manera detallada para futuros análisis. Esto permitirá revisar el desempeño del plan de contingencia y aprender de la situación para mejorar el plan de riesgos en el futuro.

7. Recuperarse de la crisis

Una vez superada la crisis, independientemente de si el plan de contingencia funcionó como estaba previsto o no, es fundamental emprender acciones de recuperación. Esta fase se centra en restablecer el equilibrio del proyecto, recompensar el esfuerzo adicional del equipo y ajustar las metas y plazos de acuerdo con los impactos sufridos.

Estrategias para Recuperarse de la Crisis:

1. Recompensar al equipo:
 - El equipo posiblemente haya tenido que trabajar bajo presión y en condiciones más duras durante la crisis. Reconocer y recompensar su esfuerzo es clave para mantener la motivación. Esto puede incluir:
 - Reconocimientos formales como elogios o menciones.
 - Compensaciones económicas o bonificaciones adicionales.



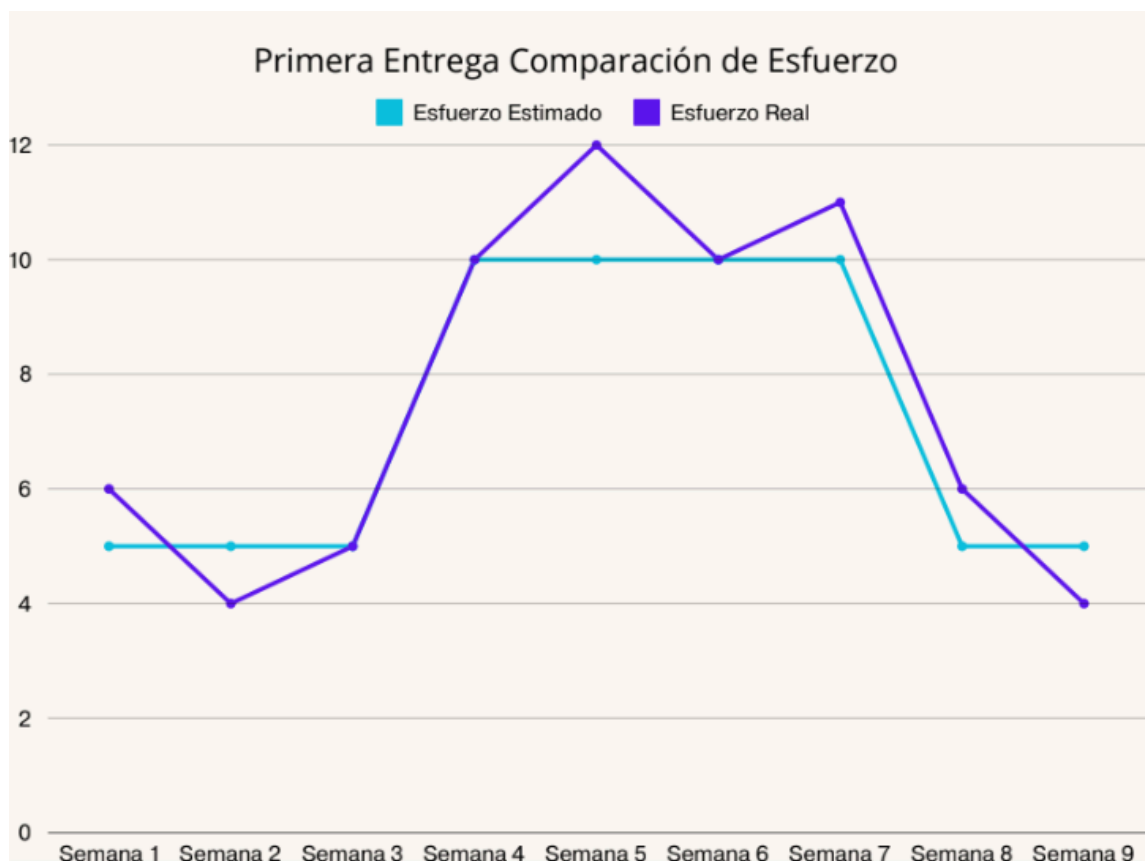
- Tiempo libre compensatorio si el equipo trabajó horas extras o fines de semana.
2. Re-planificación del proyecto:
- Una vez resuelta la crisis, el proyecto deberá ser re-planificado. Es importante ajustar tanto los plazos como los costes en función de los impactos sufridos durante la crisis.
 - Evaluar los retrasos causados por la crisis y ajustar el cronograma del proyecto.
 - Reasignar recursos si es necesario para recuperar el ritmo del proyecto.
 - Revisar los presupuestos y, si corresponde, negociar con los clientes.
3. Aprender del error/situación
- Posteriormente, el equipo debe realizar una revisión post-crisis para identificar qué aspectos del plan de contingencia funcionaron y cuáles no. Esto permitirá:
 - Mejorar los procedimientos para futuras crisis.
 - Refinar el plan de riesgos, ajustando las estrategias y medidas de mitigación para evitar la repetición de los mismos errores.
4. Recuperar la confianza del cliente:
- Si la crisis tuvo un impacto significativo en el cliente, es fundamental trabajar en restaurar la confianza. Esto incluye:
 - Informar de manera transparente sobre las acciones tomadas durante la crisis.
 - Asegurar que los problemas fueron resueltos de manera definitiva.
 - Presentar una nueva planificación que demuestre cómo se recuperarán los plazos y el presupuesto afectado.

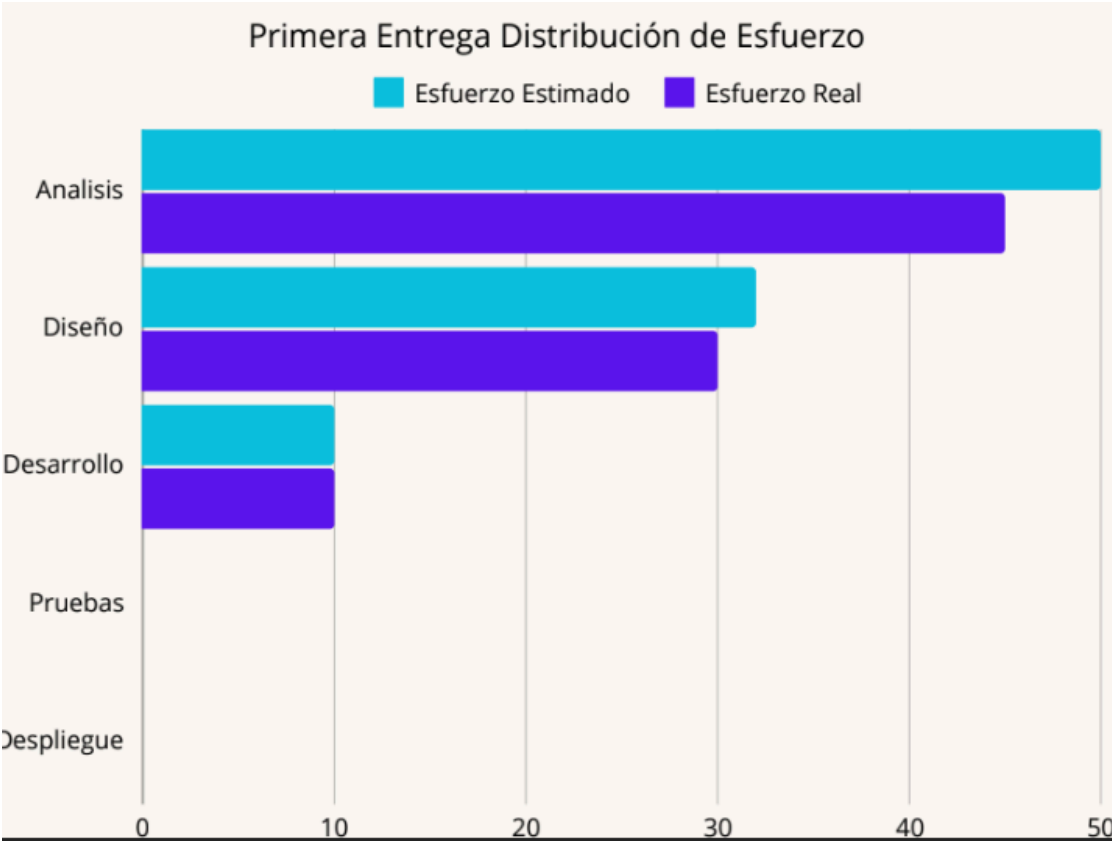
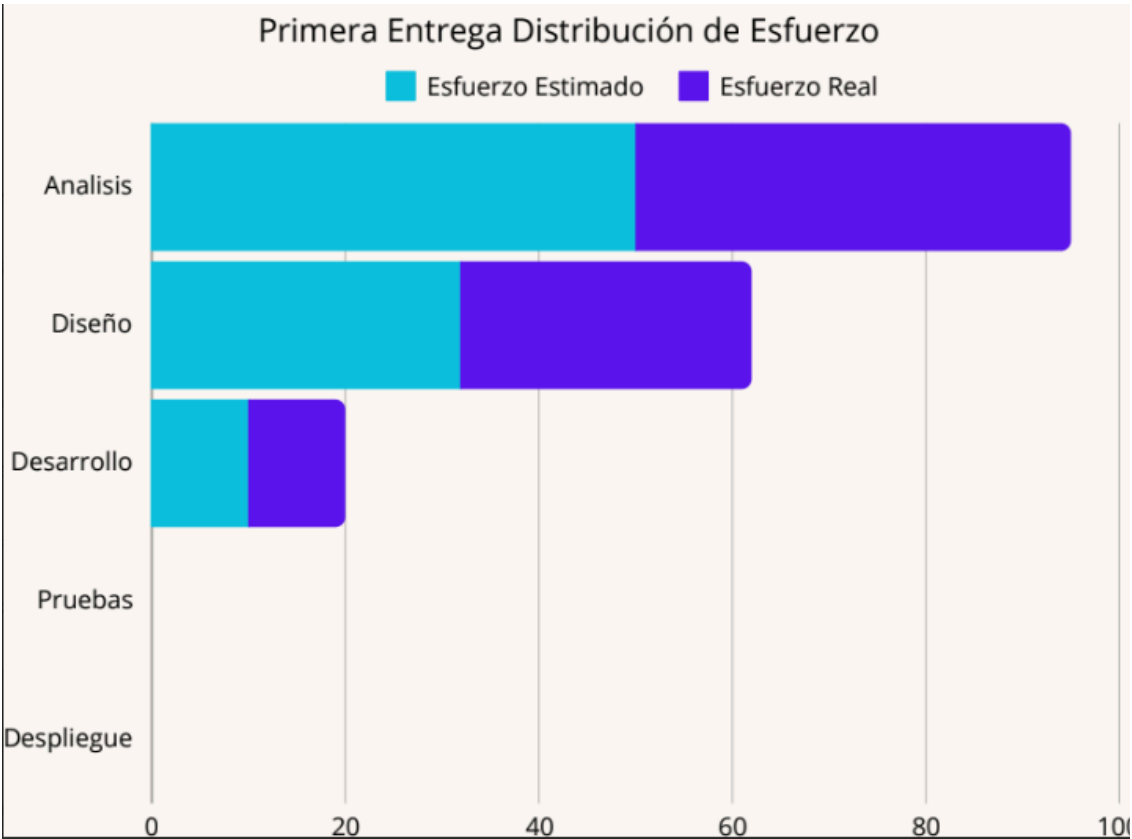


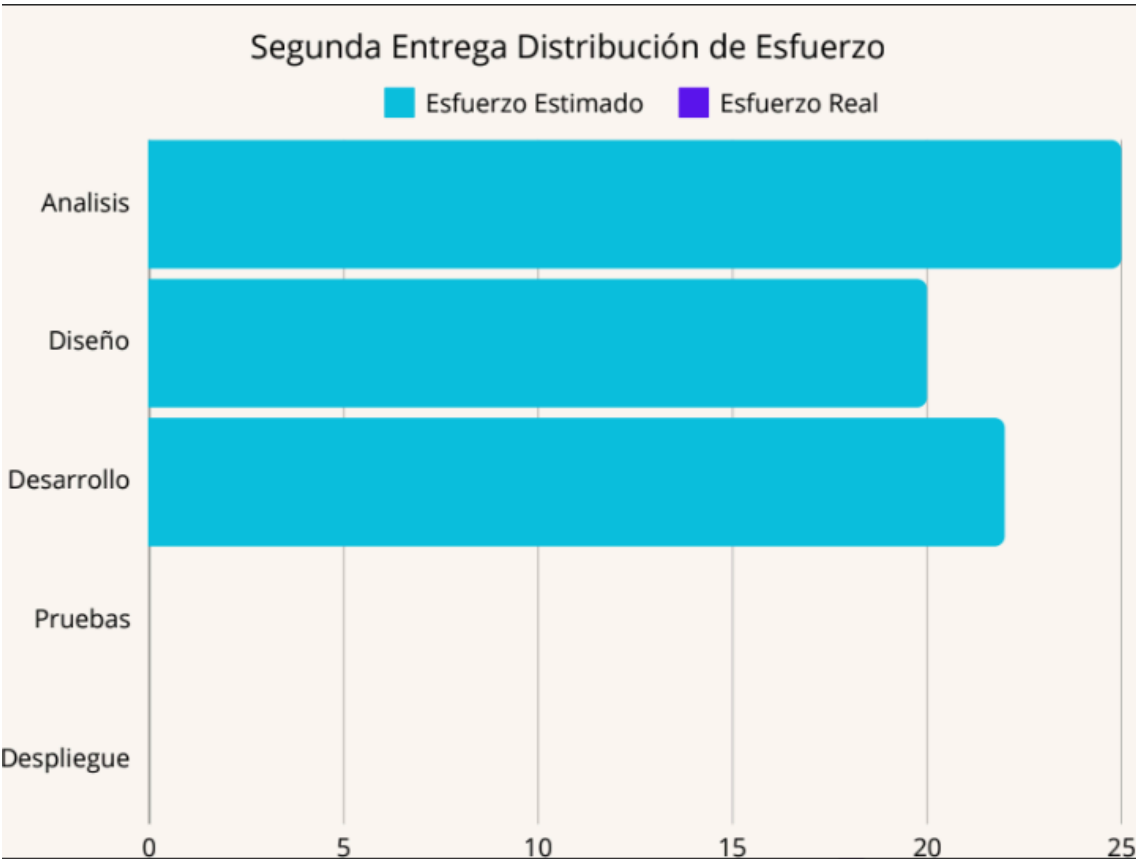
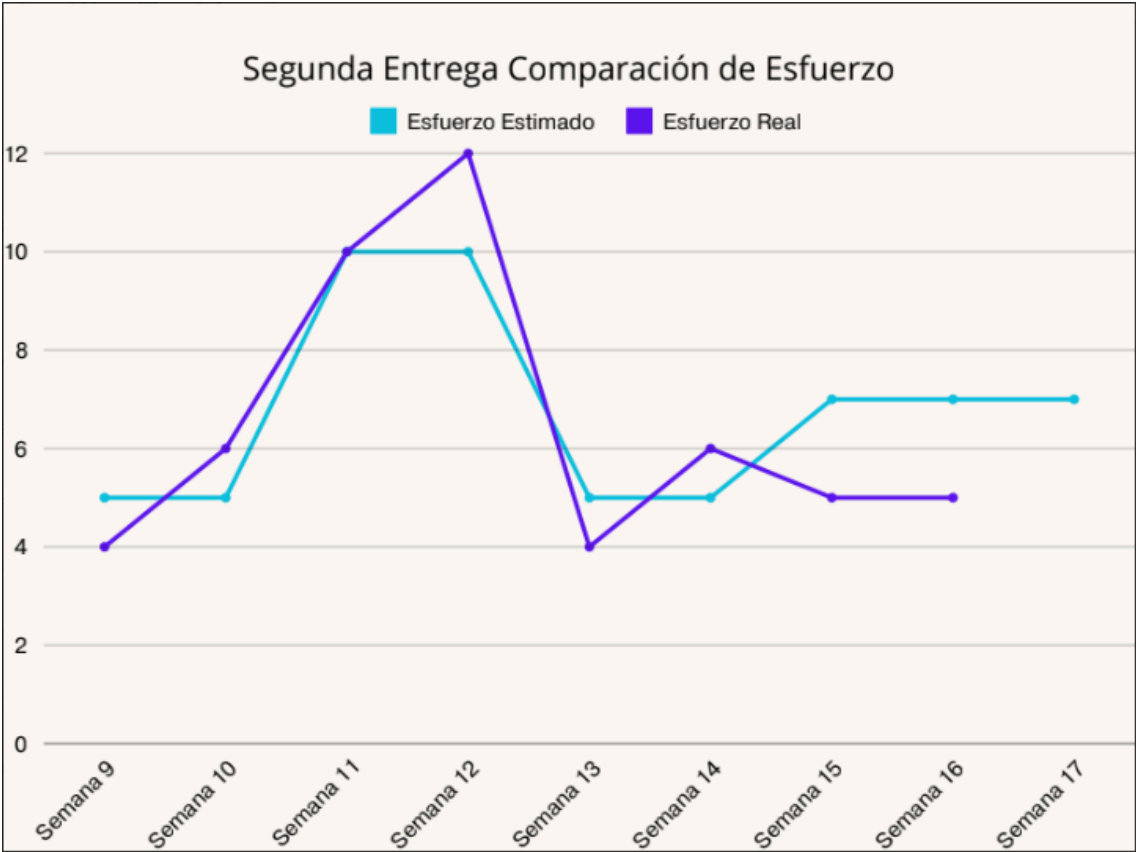
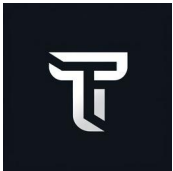
Gráficas de Esfuerzo

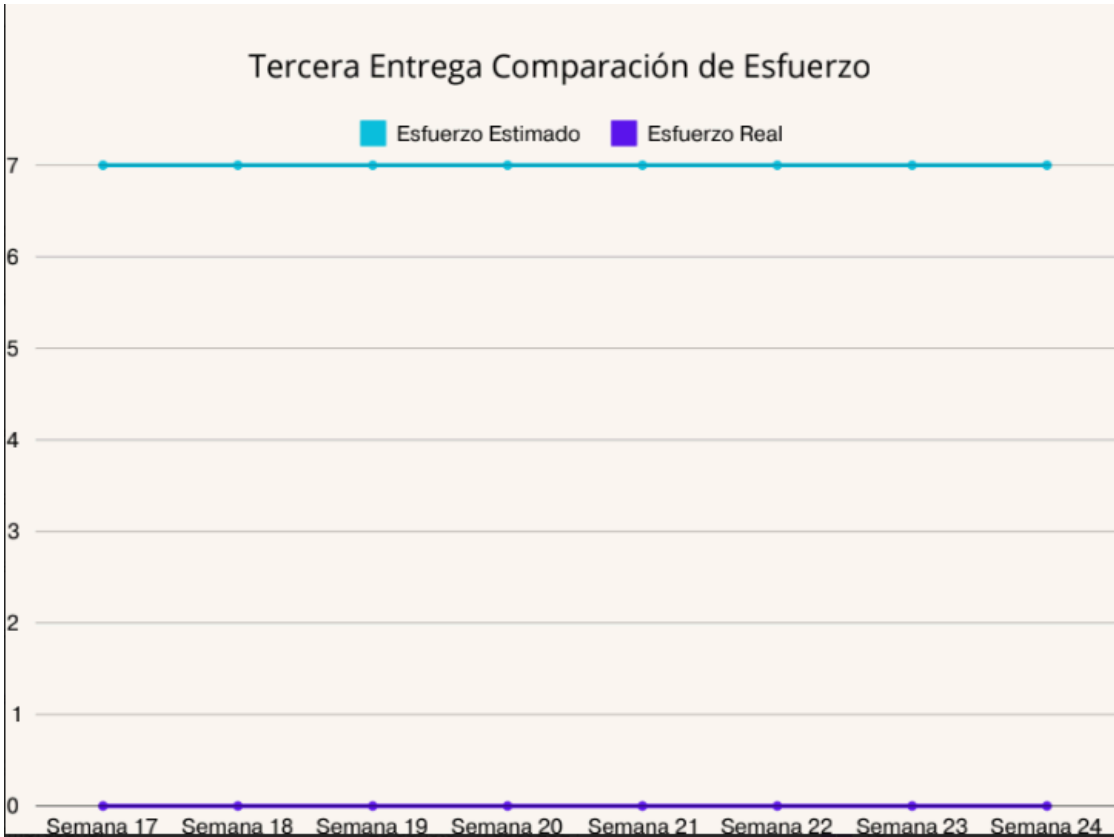
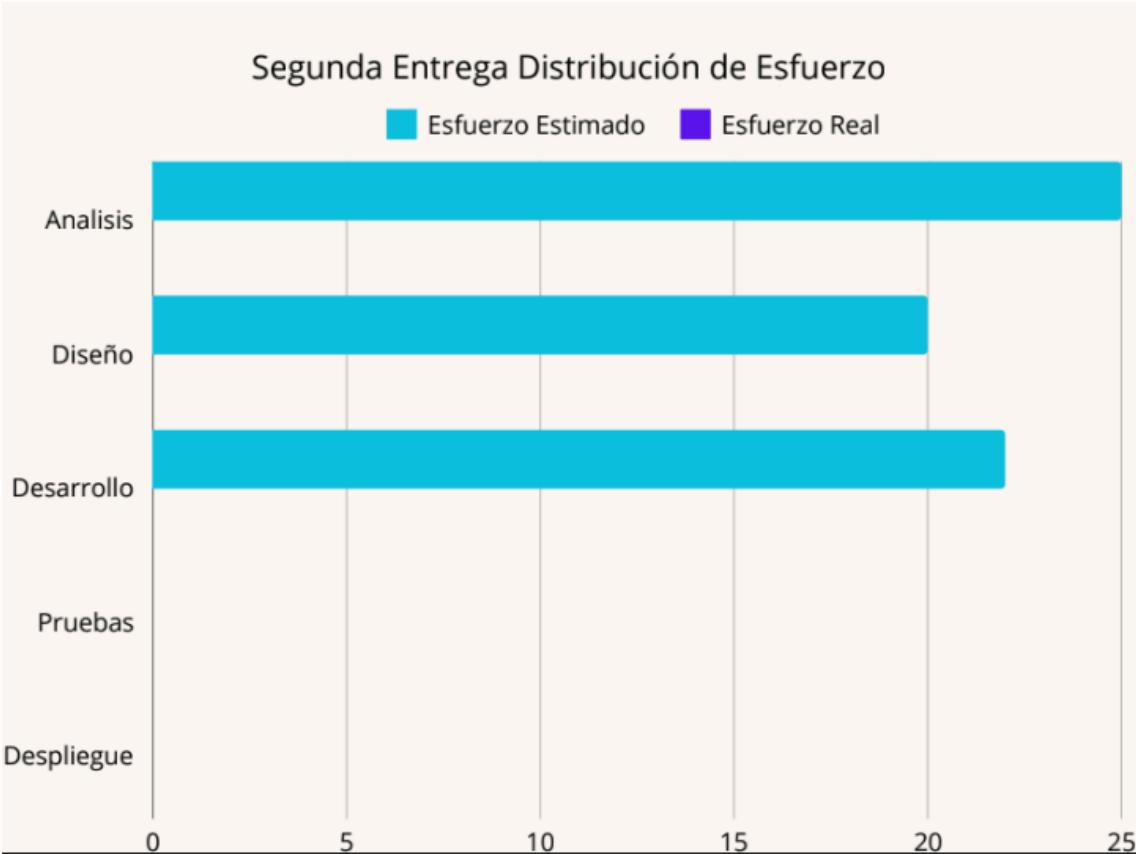
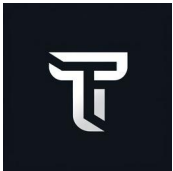
Se continuó trabajando en la gestión del proyecto. En este caso, se realizaron gráficas de esfuerzo, donde se comparan los tiempos estimados por el grupo con los tiempos reales de ejecución.

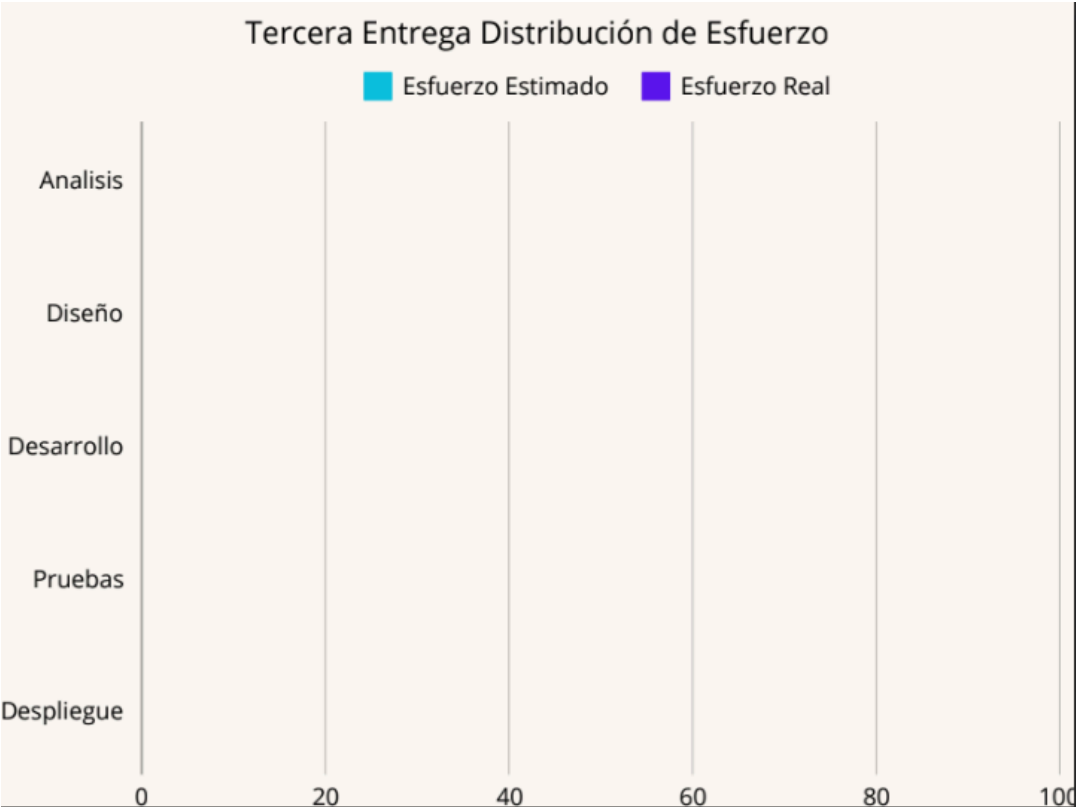
Para cada entrega del proyecto, se tomaron en cuenta tanto el tiempo planificado (en días) como el esfuerzo necesario (medido también en días o personas-días). A continuación, se muestran las gráficas (Las gráficas pertenecientes a la 3era entrega no tienen datos porque aún no se realizó).





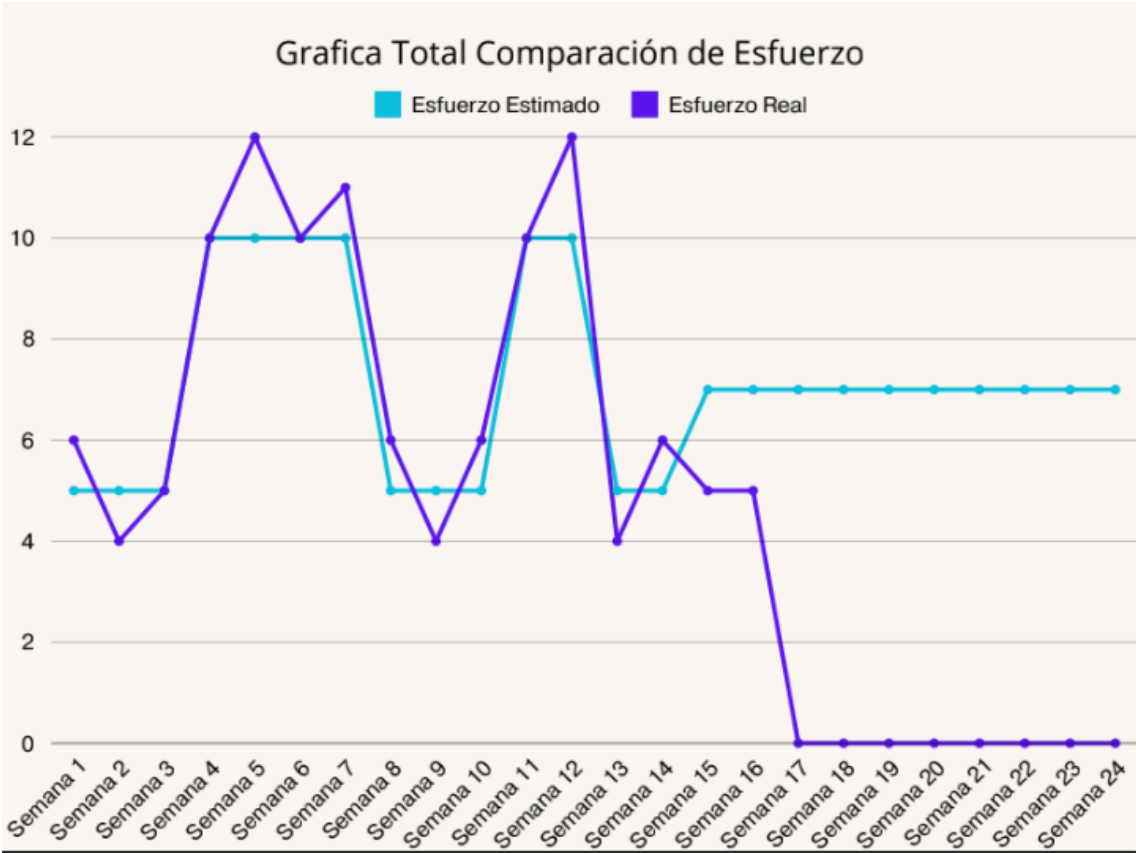


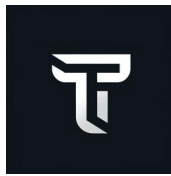






Por último tenemos la gráfica total de comparación del esfuerzo.





Actas de Reuniones (Segunda Entrega)

ESCUELA TÉCNICA ITI

24/07/2024

ACTA N°4

En la ciudad de Montevideo siendo la hora 11:05.

Se deja constancia que la reunión tuvo lugar en Instituto Tecnológico de Informática
donde se encontraban presentes Mathias Díaz, Alejo Tabares, Cristian Carpio y Brayan Rivero

Perteneciente al grupo y responsable del acta: Mathias Díaz.

Se hace constar que se trataron las siguientes tareas referidas al proyecto:

- Planificación de la segunda entrega

Firma del responsable del acta:

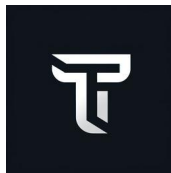
Mathias Díaz

Firma de los demás participantes:

Alejo Tabares

Cristian Carpio

Brayan Rivero



ESCUELA TÉCNICA ITI

29/07/2024

ACTA N°5

En la ciudad de Montevideo siendo la hora 19:00.

Se deja constancia que la reunión tuvo lugar en Discord
donde se encontraban presentes Mathias Díaz y Alejo Tabares

Perteneciente al grupo y responsable del acta: Mathias Díaz.

Se hace constar que se trataron las siguientes tareas referidas al proyecto:

- Boceto del sistema para implementación del mismo

Firma del responsable del acta:

Mathias Díaz

Firma de los demás participantes:

Alejo Tabares



ESCUELA TÉCNICA ITI

30/07/2024

ACTA N°6

En la ciudad de Montevideo siendo la hora 19:00

Se deja constancia que la reunión tuvo lugar en Discord
donde se encontraban presentes Mathias Díaz y Alejo Tabares

Perteneciente al grupo y responsable del acta: Mathias Díaz.

Se hace constar que se trataron las siguientes tareas referidas al proyecto:

- Continuar con el boceto del sistema para implementación del mismo

Firma del responsable del acta:

Mathias Díaz

Firma de los demás participantes:

Alejo Tabares



ESCUELA TÉCNICA ITI

13/08/2024

ACTA N°7

En la ciudad de Montevideo siendo la hora 11:05.

Se deja constancia que la reunión tuvo lugar en Instituto Tecnológico de Informática

donde se encontraban presentes Mathias Díaz, Alejo Tabares, Cristian Carpio, Dylan Arrua y Brayan Rivero

Perteneciente al grupo y responsable del acta: Mathias Díaz.

Se hace constar que se trataron las siguientes tareas referidas al proyecto:

- Script de Sistemas Operativos

Firma del responsable del acta:

Mathias Díaz

Firma de los demás participantes:

Alejo Tabares

Dylan Arrua

Cristian Carpio

Brayan Rivero



ESCUELA TÉCNICA ITI

21/08/2024

ACTA N°8

En la ciudad de Montevideo siendo la hora 11:05.

Se deja constancia que la reunión tuvo lugar en Instituto Tecnológico de Informática

donde se encontraban presentes Mathias Díaz, Alejo Tabares, Cristian Carpio y Brayan Rivero

Perteneciente al grupo y responsable del acta: Mathias Díaz.

Se hace constar que se trataron las siguientes tareas referidas al proyecto:

- Trabajos sobre Base de Datos

Firma del responsable del acta:

Mathias Díaz

Firma de los demás participantes:

Alejo Tabares

Cristian Carpio

Brayan Rivero



Anexo

Diagrama inicial KANBAN (Sin aplicar Metodología Agile)

<https://teamtryhard.atlassian.net/jira/core/projects/SIGEN/board?atlOrigin=eyJpIjoiZjZIZDZiNzJIY2E3NDQ5NWJhOTJmMDI3ZTYzNDhhMmMiLCJwIjoiaj9>

METODOLOGÍA ÁGIL CON SCRUM Y KANBAN

<https://teamtryhard.atlassian.net/jira/software/projects/SGN/boards/3/backlog>

Bibliografía

ADEN Business Magazine. (s.f.). *Metodologías ágiles: qué son, tipos y ventajas*. Recuperado el (22/8/2024), de

<https://www.aden.org/business-magazine/metodologias-agiles/>

Atlassian. (s.f.). *Kanban vs Scrum: diferencias y cuándo usar cada uno*.

Recuperado el (23/8/2024), de

<https://www.atlassian.com/es/agile/kanban/kanban-vs-scrum>

Profile. (s.f.). *Historias de usuario: qué son y cómo escribirlas correctamente*.

Recuperado el (23/8/2024), de <https://profile.es/blog/historias-de-usuario/>

Bitrix24. (s.f.). *¿Qué es un plan de contingencia? 7 pasos para una planificación de contingencia sólida para tu empresa*. Recuperado el (15/8/2024), de

<https://www.bitrix24.es/articles/que-es-un-plan-de-contingencia-7-pasos-para-una-planificacion-de-contingencia-solida-para-tu-empresa.php#:~:text=Un%20plan%20de%20contingencia%20es%20un%20conjunto%20de%20medidas%20y,estrategias%20de%20recuperaci%C3%B3n%20ante%20desastres>.

Escuela Europea de Excelencia. (2022, noviembre). *Cómo redactar planes de gestión de riesgos y por qué hacerlo es importante*. Recuperado el [2/9/2024], de



<https://www.escuelaeuropeaexcelencia.com/2022/11/como-redactar-planes-de-gestion-de-riesgos-y-por-que-hacerlo-es-importante/#:~:text=Un%20plan%20de%20gesti3n%20de%20riesgos%20es%20un%20documento%20en,negativo%20o%20aprovechar%20posibles%20oportunidades>.