FACULTAD
DE INGENIERIA
Universidad de Buenos Aires

Sistema de Aislamiento Limitado/Total Ferroviario

Autor:
Ing. Nahuel Espinosa

Director:
Dr. Ing. Pablo Gomez (CONICET-GICSAFe)

Jurados:
Nombre y Apellido (1) (pertenencia (1))
Nombre y Apellido (2) (pertenencia (2))
Nombre y Apellido (3) (pertenencia (3))

Este trabajo fue realizado en el curso de Gestión de proyectos entre el 22 de junio de 2020 y el 22 de Agosto de 2020.

Índice

Registros de cambios

Revisión	Detalles de los cambios realizados	Fecha
1.0	Creación del documento	22/06/2020

Acta de Constitución del Proyecto

Buenos Aires, 22 de junio de 2020

Por medio de la presente se acuerda con el Ing. Nahuel Espinosa que su Trabajo Final de la Carrera de Especialización en Sistemas Embebidos se titulará "Sistema de Aislamiento Limitado/Total Ferroviario", consistirá esencialmente en el prototipo de un equipo que permita inhabilitar las señales de corte de tracción y frenado de emergencia en el caso de una falla en uno de los subsistemas de seguridad de una formación ferroviaria, y tendrá un presupuesto preliminar estimado de 650 hs de trabajo y $XXX, con fecha de inicio 22 de junio de 2020 y fecha de presentación pública 22 de diciembre de 2020.

Se adjunta a esta acta la planificación inicial.

Dr. Ing. Ariel Lutenberg
Director posgrado FIUBA

Ing. Alejandro Leonetti
SOFSE

Dr. Ing. Pablo Gomez
Director del Trabajo Final

Nombre y Apellido (1)
Jurado del Trabajo Final

Nombre y Apellido (2)
Jurado del Trabajo Final

Nombre y Apellido (3)
Jurado del Trabajo Final

Descripción técnica-conceptual del Proyecto a realizar

Las formaciones ferroviarias cuentan con diferentes sistemas de seguridad a bordo. Los mismos son equipos que se encargan de supervisar el correcto funcionamiento de los subsistemas críticos. Ejemplos de los mismos son la seguridad de puertas, el sistema de hombre vivo y la protección de coche a la deriva.

Ante una falla en uno de estos subsistemas, una formación ferroviaria se detiene inmediatamente por la activación automática de las señales de corte de tracción y frenado de emergencia. En esta situación el conductor debe llevar a la formación a un lugar seguro para que los pasajeros puedan descender y posteriormente a un taller para que pueda ser reparada.

En el año 2017, la empresa estatal Trenes Argentinos Operaciones (SOFSE) encargó al CONICET-GICSAFe el desarrollo de un equipo que le permita al conductor inhabilitar las señales de corte de tracción (CT) y frenado de emergencia (FE) sin comprometer la seguridad de la formación y sus pasajeros. Este equipo se conoce en el ámbito local como Sistema de Aislamiento Limitado/Total (SAL/T) y se considera un sistema crítico debido a que, en caso de fallar, puede ocasionar daños afectando negativamente la salud de las personas, al medio ambiente y/o generar grandes pérdidas materiales.

En el año 2019 se concluyó el desarrollo de un prototipo funcional del SAL/T en el marco del trabajo de tesis del Ing. Ivan Di Vito. En la Figura 1 se puede ver como interactúa con las señales CT y FE. En modo de funcionamiento normal los subsistemas de seguridad tienen conexión directa con el control central. Ante la activación por parte del conductor del modo aislado limitado (AL) el SAL/T toma el control de dichas señales.

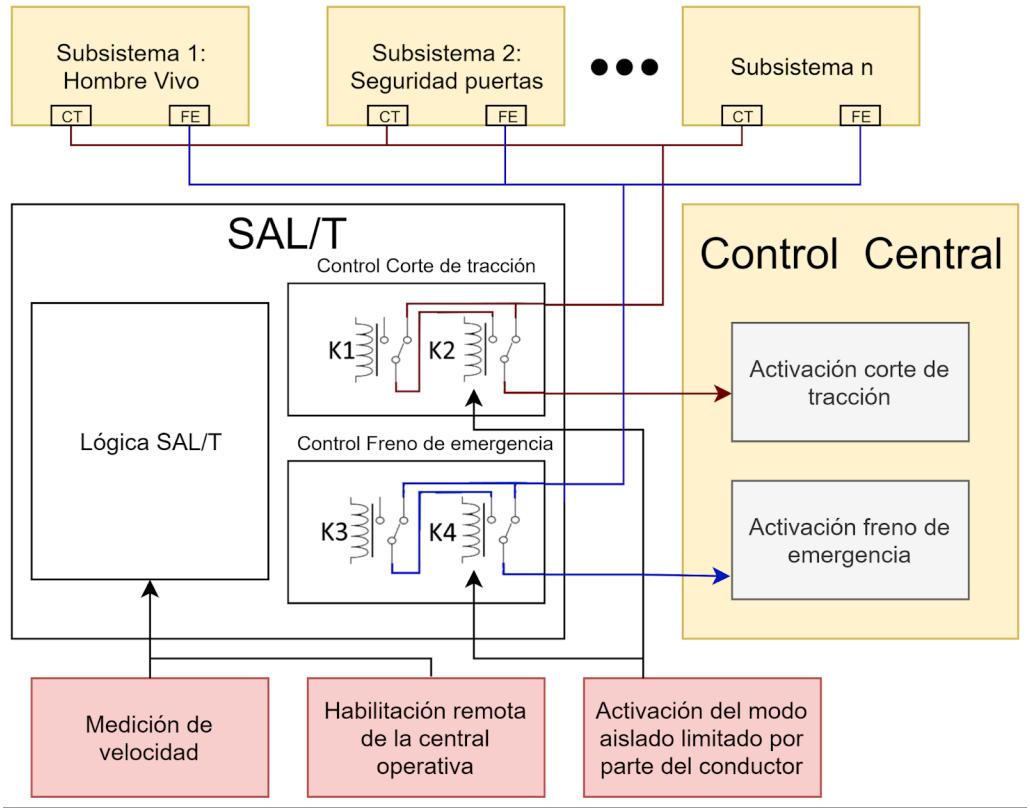

Figura 1: Diagrama conceptual de la interacción del SAL/T con los sistemas de seguridad en una formación.

El SAL/T monitorea la velocidad de la formación e informa su estado interno al registrador de eventos Hasler Teloc 1500 y a una central operativa, a través de un enlace de comunicación redundado, de la cual también puede recibir comandos remotos que modifiquen su comportamiento.

En la Figura 2 se resaltan las cinco primeras fases completadas del ciclo de vida propuesto por la norma UNE-EN 50126 para aplicaciones ferroviarias. La documentación de la sexta fase, que corresponde al diseño e implementación del sistema, y las fases posteriores quedaron fuera del alcance del trabajo original.

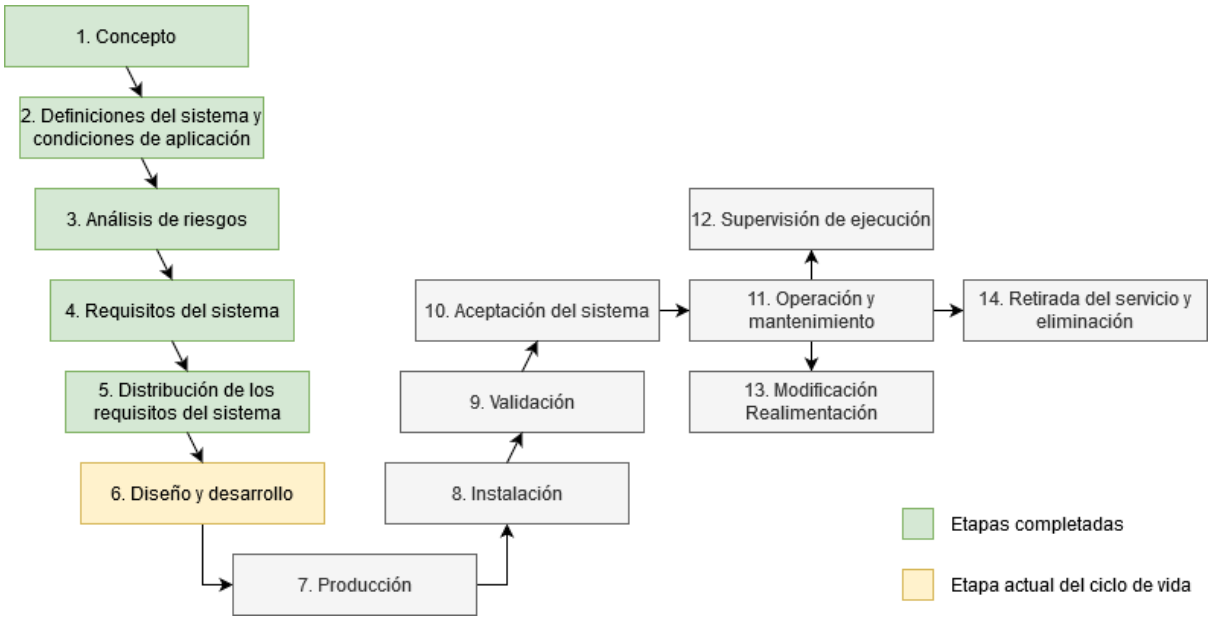

Figura 2: Ciclo de vida de un sistema propuesto por la norma UNE-EN 50126.

Este proyecto continuará con el desarrollo del SAL/T revisando los requisitos de seguridad RAMS establecidos en la cuarta fase del trabajo original, diseñando subsistemas que se ajusten a los requisitos y verificando el nivel de integridad de seguridad (SIL).

Para el caso específico de los sistemas eléctrico-programables (EP) la fase de diseño y desarrollo se divide en dos partes relacionadas con el desarrollo del hardware y del software.

- El diseño del software buscará seguir una metodología acorde a la norma UNE-EN 50128 centrada en la calidad de los aspectos de software de los sistemas de ferrocarriles.
- En el nuevo diseño de la placa principal se reemplazará la plataforma EDU-CIAA-NXP, utilizada como base en la primera versión, por un módulo ad-hoc de procesamiento.

Identificación y análisis de los interesados

Rol	Nombre y Apellido	Organización	Puesto
Cliente	Ing. Alejandro Leonetti	SOFSE	Gerente de Seguridad Operacional
Responsable	Ing. Nahuel Espinosa	FIUBA	Alumno
Colaboradores	Dr. Ing. Ariel Lutenberg	CONICET-GICSAFe	Director Grupo de Investigación
Orientador	Dr. Ing. Pablo Gomez	CONICET-GICSAFe	Director Trabajo final

1. Propósito del proyecto

El propósito de este proyecto es continuar el desarrollo de un sistema de supervisión de seguridad de formaciones ferroviarias denominado SAL/T (Sistema de Aislamiento Limitado/Total) que alcance niveles RAMS adecuados para su uso a criterio de las autoridades SOFSE y CNRT.

2. Alcance del proyecto

El desarrollo del presente proyecto incluye:

- Revisión y actualización de la documentación generada en las primeras cinco fases del ciclo de vida del proyecto original.
- Diseño, implementación y documentación del firmware siguiendo la norma UNE-EN 50128 utilizando herramientas de integración y ensayos.
- Diseño y fabricación de una nueva versión de la placa principal del hardware reemplazando la EDU-CIAA-NXP por un procesador ad-hoc.
- Verificación del nivel de integridad de seguridad (SIL) del sistema.

El presente proyecto NO incluye:

- Desarrollo de la séptima fase y posteriores del ciclo de vida del proyecto (producción, instalación, validación, etc.).
- Desarrollo del software necesario para la central operativa.
- Modificación del gabinete.
- Certificación de los sistemas a ser desarrollados.

3. Supuestos del proyecto

Para el desarrollo del presente proyecto se supone que:

- Es posible continuar el proyecto a partir del análisis, la definición de subsistemas e interacciones y el uso de patrones de diseño del trabajo original.
- Se tendrá acceso al prototipo actual para hacer pruebas de integridad con el nuevo firmware.
- Una vez finalizado el diseño del PCB, se podrá fabricar el mismo en un tiempo razonable.
- No habrá dificultades para conseguir los componentes electrónicos necesarios.
- Se adquirirán los conocimientos necesarios sobre la normativa aplicable.
- El tiempo estipulado será suficiente para alcanzar los objetivos definidos.

4. Requerimientos

Estos requerimientos fueron obtenidos a partir de los documentos "R_DCP_10 Definición Conceptual del Proyecto - Fase 1" y "R_DRQ_10 Distribución de los requisitos del sistema - Fase 5". Los mismos fueron creados originalmente por el Ing. Ivan Di Vito siguiendo la recomendación de la norma UNE-EN 50126 como resultado de múltiples reuniones con las diferentes partes interesadas en la realización del proyecto.

Esas reuniones incluyeron la participación de personal de SOFSE de la Gerencia de Seguridad Operacional, del departamento de material rodante y de personal de los talleres de reparación y mantenimiento de Liniers y Victoria. También participó personal de la Comisión Nacional de Regulación del Transporte (CNRT).

Se estudió la documentación original teniendo en cuenta el estado actual del prototipo y se redactaron los requerimientos agrupándolos por afinidad:

1. Grupo de requerimientos asociados con la interfaz humano-máquina
   - 1.1. La interfaz debe contar con una llave rotativa precintable para activar el modo aislado limitado.
   - 1.2. La interfaz debe indicar el modo actual del sistema (modo aislado o modo normal).
   - 1.3. La interfaz debe mostrar la velocidad media del equipo en km/h (3 ó 4 dígitos).
   - 1.4. La interfaz debe indicar el estado de las señales de corte de tracción y freno de emergencia.
   - 1.5. La interfaz debe indicar la presencia de un comando remoto de la central operativa.
   - 1.6. La interfaz debe indicar el estado de los módulos GPS.
2. Grupo de requisitos asociados a la comunicación con el registrador de eventos
   - 2.1. El sistema debe informar al registrador de eventos la activación del modo aislado limitado.
   - 2.2. El sistema debe informar al registrador de eventos si la alimentación es correcta.
   - 2.3. El sistema debe informar al registrador de eventos la activación del freno de emergencia.
   - 2.4. El sistema debe informar al registrador de eventos la activación del corte de tracción.
3. Grupo de requisitos asociados a la comunicación con la central operativa
   - 3.1. El sistema debe informar periódicamente (con un tiempo configurable) su estado a la central operativa a través de la red de datos GPRS, 3G ó 4G.
   - 3.2. El sistema debe utilizar la antena GPRS/GPS ya disponible en la formación.
   - 3.3. Debe existir la posibilidad de usar 2 proveedores distintos de datos de manera simultánea.
   - 3.4. El protocolo de comunicación con la central operativa debe ser MQTT.
   - 3.5. El sistema debe ser capaz de recibir un comando remoto que anule el corte de tracción y el freno de emergencia bajo cualquier condición (modo aislado total).
   - 3.6. El sistema debe ser capaz de recibir un comando remoto que active el corte de tracción y el freno de emergencia bajo cualquier condición (modo parada total).

3.7. El sistema debe ser capaz de recibir un comando remoto que active el corte de tracción y anule el freno de emergencia bajo cualquier condición (modo coche en deriva).

3.8. El sistema debe ser capaz de recibir un comando remoto que active el corte de tracción y el freno de emergencia de forma intermitente en ciclos de tiempo configurables (modo intermitente).

3.9. El sistema debe ser capaz de recibir un comando remoto que cancele cualquier comando remoto vigente (exit).

3.10. El sistema debe ser capaz de recibir comandos remotos que modifiquen sus parámetros internos configurables.

3.11. Si no se recibe un nuevo comando remoto luego de un tiempo configurable (por defecto 10 segundos, máximo 1 minuto), debe volver al algoritmo de activación de corte de tracción y freno de emergencia por defecto.

3.12. Ante un comando remoto recibido, debe enviar una confirmación de recepción que permita a la central operativa decidir si es necesaria o no una retransmisión.

3.13. Debe utilizar algún mecanismo de encriptación para el enlace con la central operativa.

4. Grupo de requerimientos asociados al modo normal de funcionamiento

4.1. EL modo normal no debe intervenir en el funcionamiento del material rodante (prioridad alta).

4.2. El sistema debe obtener en todo momento la mejor estimación posible de la velocidad de la formación.

4.2.1 Debe ser capaz de recibir la velocidad a partir de una señal digital provista por el registrador de eventos Hasler Teloc 1500.

4.2.2 Debe ser capaz de calcular la velocidad a partir de un generador de impulsos ópticos instalado en una o varias ruedas de la formación.

4.2.3 Debe ser capaz de calcular la velocidad a partir de un sistema GPS integrado.

4.3. El rango de velocidad soportado por el sistema tiene que estar entre 0 y 120 km/h.

4.4. La estimación de velocidad debe tener una precisión del 2 % de fondo de escala.

5. Grupo de requerimientos asociados al modo aislado limitado

5.1. En modo aislado limitado el sistema debe evitar la aplicación del corte de tracción y/o freno de emergencia por parte de los subsistemas de seguridad del material rodante.

5.2. En modo aislado limitado el sistema debe emitir una señal sonora intermitente a través de un buzzer.

5.3. En modo aislado limitado el sistema debe evitar que la velocidad del material rodante supere una serie de límites configurados.

5.3.1 Si al pasar de modo normal a modo aislado limitado no se cuenta con una estimación de velocidad, debe activar el corte de tracción y el freno de emergencia por 30 segundos.

5.3.2 Si se supera una velocidad configurable (por defecto 30 km/h), debe activar el corte de tracción y emitir una señal sonora continua a través de un buzzer.

5.3.3 Si se supera una velocidad configurable (por defecto 36 km/h), debe activar el freno de emergencia.

5.3.4 Una vez aplicado, el corte de tracción debe dejar de aplicarse si la velocidad vuelve a ser menor a una velocidad configurable (por defecto 25 km/h).

5.3.5 Una vez aplicado, el freno de emergencia sólo debe dejar de aplicarse luego de un tiempo configurable (por defecto 30 segundos) desde que se superó el límite.

5.3.6 Si la lectura de velocidad es inválida, debe activar y desactivar el corte de tracción y freno de emergencia de manera alternada en ciclos de tiempo configurables.

6. Grupo de requerimientos asociados al hardware y al gabinete

6.1. El sistema debe utilizar la alimentación presente en el material rodante compredida entre 72 V y 100 V.

6.2. Los conectores deben ser unívocos imposibilitando la conexión incorrecta.

6.3. Debe poseer una única placa para el procesamiento principal.

6.4. Debe estar diseñado para ser instalado en la locomotora sobre el pupitre.

6.5. El gabinete debe tener grado de seguridad IP66 o superior.

5. Entregables principales del proyecto

- Código fuente y documentación del firmware
- Diagramas esquemáticos del circuito impreso
- Archivos para fabricación del circuito impreso
- Informe de avance
- Informe final

6. Desglose del trabajo en tareas

1.	Planificación del proyecto	(total 20 hs)
1.1.	Elaboración del plan de proyecto	(20 hs)
2.	Investigación preliminar	(total 90 hs)
2.1.	Estudio de la documentación original	(40 hs)
2.2.	Estudio de la arquitectura y el código fuente original	(20 hs)
2.3.	Estudio de la normativa	(30 hs)
3.	Desarrollo del firmware	(total 290 hs)
3.1.	Identificación y desarrollo de aspectos de la normativa	(20 hs)
3.2.	Revisión y actualización de la arquitectura del firmware	(20 hs)
3.3.	Selección y configuración del entorno de desarrollo	(10 hs)
3.4.	Selección de librerías externas	(10 hs)
3.5.	Implementación de drivers y primitivas	(20 hs)
3.6.	Implementación de módulo de interfaz hombre-máquina	(30 hs)
3.7.	Implementación de módulo de medición de velocidad	(40 hs)
3.8.	Implementación de módulo de comunicación y localización	(40 hs)
3.9.	Implementación de módulo de lógica principal (modos de funcionamiento)	(40 hs)
3.10.	Definición de casos de prueba	(20 hs)

3.11. Pruebas y validación del firmware (40 hs)

4. Desarrollo del hardware (total 130 hs)
   - 4.1. Selección de módulos y componentes (10 hs)
   - 4.2. Actualización de los diagramas esquemáticos (20 hs)
   - 4.3. Diseño del circuito impreso (60 hs)
   - 4.4. Pruebas y validación del hardware (40 hs)
5. Integración del sistema (total 70 hs)
   - 5.1. Integración de módulos constitutivos (40 hs)
   - 5.2. Pruebas de integración y funcionalidad (20 hs)
   - 5.3. Pruebas de campo (10 hs)
6. Procesos de finalización (total 60 hs)
   - 6.1. Elaboración del informe de avance (10 hs)
   - 6.2. Elaboración de la memoria del proyecto (40 hs)
   - 6.3. Preparación de la presentación final (10 hs)

Cantidad total de horas: (660 hs)

7. Diagrama de Activity On Node

Armar el AoN a partir del WBS definido en la etapa anterior.

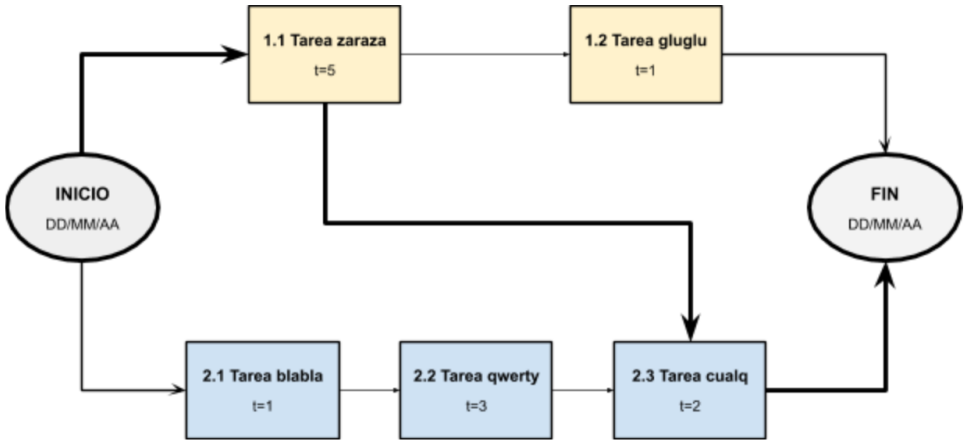

Figura 3: Diagrama en *Activity on Node*

Indicar claramente en qué unidades están expresados los tiempos. De ser necesario indicar los caminos semicríticos y analizar sus tiempos mediante un cuadro. Es recomendable usar colores y un cuadro indicativo describiendo qué representa cada color, como se muestra en el siguiente ejemplo:

8. Diagrama de Gantt

Utilizar el software Gantter for Google Drive o alguno similar para dibujar el diagrama de Gantt.

Existen muchos programas y recursos *online* para hacer diagramas de gantt, entre las cuales destacamos:

- Planner
- GanttProject
- Trello + *plugins*. En el siguiente link hay un tutorial oficial:
  `https://blog.trello.com/es/diagrama-de-gantt-de-un-proyecto`
- Creately, herramienta online colaborativa.
  `https://creately.com/diagram/example/ieb3p3ml/LaTeX`
- Se puede hacer en latex con el paquete *pgfgantt*
  `http://ctan.dcc.uchile.cl/graphics/pgf/contrib/pgfgantt/pgfgantt.pdf`

Pegar acá una captura de pantalla del diagrama de Gantt, cuidando que la letra sea suficientemente grande como para ser legible. Si el diagrama queda demasiado ancho, se puede pegar primero la "tabla" del Gantt y luego pegar la parte del diagrama de barras del diagrama de Gantt.

Configurar el software para que en la parte de la tabla muestre los códigos del EDT (WBS).
Configurar el software para que al lado de cada barra muestre el nombre de cada tarea.
Revisar que la fecha de finalización coincida con lo indicado en el Acta Constitutiva.

En la figura 4, se muestra un ejemplo de diagrama de gantt realizado con el paquete de *pgfgantt*. En la plantilla pueden ver el código que lo genera y usarlo de base para construir el propio.

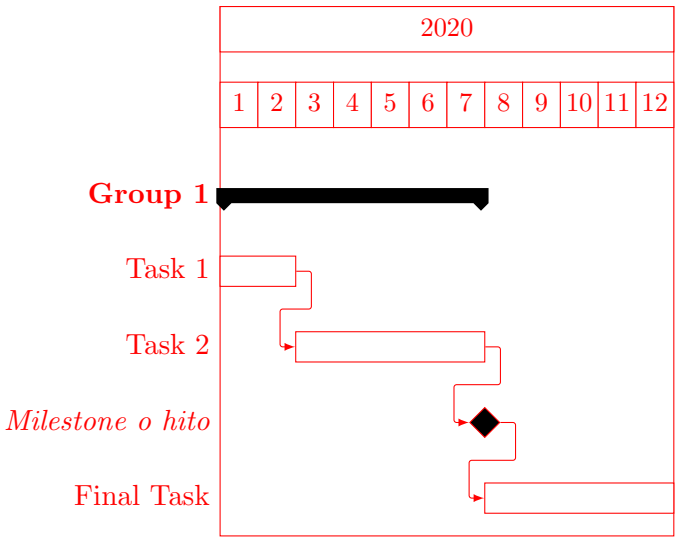

Figura 4: Diagrama de gantt de ejemplo

9. Matriz de uso de recursos de materiales

Código WBS	Nombre tarea	Recursos requeridos (horas)			
		Material 1	Material 2	Material 3	Material 4

10. Presupuesto detallado del proyecto

Si el proyecto es complejo entonces separarlo en partes:

- Un total global, indicando el subtotal acumulado por cada una de las áreas.
- El desglose detallado del subtotal de cada una de las áreas.

IMPORTANTE: No olvidarse de considerar los COSTOS INDIRECTOS.

COSTOS DIRECTOS			
Descripción	Cantidad	Valor unitario	Valor total
SUBTOTAL			
COSTOS INDIRECTOS			
Descripción	Cantidad	Valor unitario	Valor total
SUBTOTAL			
TOTAL			

11. Matriz de asignación de responsabilidades

Establecer la matriz de asignación de responsabilidades y el manejo de la autoridad completando la siguiente tabla:

Código WBS	Nombre de la tarea	Listar todos los nombres y roles del proyecto			
		Responsable	Orientador	Equipo	Cliente
		Ing. Nahuel Espinosa	Dr. Ing. Pablo Gomez	Nombre de alguien	Ing. Alejandro Leonetti

Referencias:

- P = Responsabilidad Primaria

- S = Responsabilidad Secundaria
- A = Aprobación
- I = Informado
- C = Consultado

Una de las columnas debe ser para el Director, ya que se supone que participará en el proyecto. A su vez se debe cuidar que no queden muchas tareas seguidas sin "A" o "I".

Importante: es redundante poner "I/A" o "I/C", porque para aprobarlo o responder consultas primero la persona debe ser informada.

12. Gestión de riesgos

a) Identificación de los riesgos (al menos cinco) y estimación de sus consecuencias:

Riesgo 1: detallar el riesgo (riesgo es algo que si ocurre altera los planes previstos)

- Severidad (S): mientras más severo, más alto es el número (usar números del 1 al 10). Justificar el motivo por el cual se asigna determinado número de severidad (S).
- Probabilidad de ocurrencia (O): mientras más probable, más alto es el número (usar del 1 al 10).
  Justificar el motivo por el cual se asigna determinado número de (O).

Riesgo 2:

- Severidad (S):
- Ocurrencia (O):

Riesgo 3:

- Severidad (S):
- Ocurrencia (O):

b) Tabla de gestión de riesgos: (El RPN se calcula como RPN=SxO)

Riesgo	S	O	RPN	S*	O*	RPN*

Criterio adoptado: Se tomarán medidas de mitigación en los riesgos cuyos números de RPN sean mayores a ....

Nota: los valores marcados con (*) en la tabla corresponden luego de haber aplicado la mitigación.

c) Plan de mitigación de los riesgos que originalmente excedían el RPN máximo establecido:

Riesgo 1: Plan de mitigación (si por el RPN fuera necesario elaborar un plan de mitigación). Nueva asignación de S y O, con su respectiva justificación: - Severidad (S): mientras más severo, más alto es el número (usar números del 1 al 10). Justificar el motivo por el cual se asigna determinado número de severidad (S). - Probabilidad de ocurrencia (O): mientras más probable, más alto es el número (usar del 1 al 10). Justificar el motivo por el cual se asigna determinado número de (O).

Riesgo 2: Plan de mitigación (si por el RPN fuera necesario elaborar un plan de mitigación).

Riesgo 3: Plan de mitigación (si por el RPN fuera necesario elaborar un plan de mitigación)

13. Gestión de la calidad

Para cada uno de los requerimientos del proyecto indique:

- Req #1: Copiar acá el requerimiento.
  Verificación y validación:
  - Verificación para confirmar si se cumplió con lo requerido antes de mostrar el sistema al cliente:
    Detallar
  - Validación con el cliente para confirmar que está de acuerdo en que se cumplió con lo requerido:
    Detallar

Tener en cuenta que en este contexto se pueden mencionar simulaciones, cálculos, revisión de hojas de datos, consulta con expertos, etc.

14. Comunicación del proyecto

El plan de comunicación del proyecto es el siguiente:

PLAN DE COMUNICACIÓN DEL PROYECTO					
¿Qué comunicar?	Audiencia	Propósito	Frecuencia	Método de comunicac.	Responsable

15. Gestión de Compras

En caso de tener que comprar elementos o contratar servicios: a) Explique con qué criterios elegiría a un proveedor. b) Redacte el Statement of Work correspondiente.

16. Seguimiento y control

Para cada tarea del proyecto establecer la frecuencia y los indicadores con los se seguirá su avance y quién será el responsable de hacer dicho seguimiento y a quién debe comunicarse la situación (en concordancia con el Plan de Comunicación del proyecto).

El indicador de avance tiene que ser algo medible, mejor incluso si se puede medir en % de avance. Por ejemplo,se pueden indicar en esta columna cosas como "cantidad de conexiones ruteadeas" o "cantidad de funciones implementadas", pero no algo genérico y ambiguo como "%", porque el lector no sabe porcentaje de qué cosa.

SEGUIMIENTO DE AVANCE					
Tarea del WBS	Indicador de avance	Frecuencia de reporte	Resp. de seguimiento	Persona a ser informada	Método de comunic.

17. Procesos de cierre

Establecer las pautas de trabajo para realizar una reunión final de evaluación del proyecto, tal que contemple las siguientes actividades:

- Pautas de trabajo que se seguirán para analizar si se respetó el Plan de Proyecto original: - Indicar quién se ocupará de hacer esto y cuál será el procedimiento a aplicar.
- Identificación de las técnicas y procedimientos útiles e inútiles que se utilizaron, y los problemas que surgieron y cómo se solucionaron: - Indicar quién se ocupará de hacer esto y cuál será el procedimiento para dejar registro.
- Indicar quién organizará el acto de agradecimiento a todos los interesados, y en especial al equipo de trabajo y colaboradores: - Indicar esto y quién financiará los gastos correspondientes.