

Plantilla: Acuerdos de equipo + Plan de comunicación

Unidad 2 (RAP2) – Gestión de equipos multidisciplinarios, comunicación y coordinación

Propósito: documentar acuerdos operativos del equipo de proyecto y establecer un plan de comunicación para asegurar coordinación, adopción y control de riesgos (IA/ciberseguridad). Complete los campos y adjunte evidencias cuando aplique.

1. Información general del proyecto

Nombre del proyecto:			Código/Versión:	
Organización/Área:			Fecha:	2025-11-30
Patrocinador (Sponsor):			Líder del proyecto:	
Tipo de proyecto:	<input checked="" type="checkbox"/> IA <input checked="" type="checkbox"/> Ciberseguridad <input checked="" type="checkbox"/> Híbrido		Duración estimada:	
Objetivo (resumen):				

2. Equipo del proyecto y roles (multidisciplinario)

Incluya a los actores clave. Si un rol no existe formalmente, indique quién asume esa función.

3. Matriz RACI (mínimo 6 actividades clave)

R: Responsable (ejecuta) | A: Aprobador (autoriza) | C: Consultado | I: Informado

4. Acuerdos de equipo (Working Agreements)

Complete los acuerdos y publíquelos en el espacio del curso/proyecto. Estos acuerdos son obligatorios para reducir retrabajo, mejorar coordinación y gestionar riesgos de datos y seguridad.

4.1 Canales y reglas de comunicación

Canal oficial del proyecto (ej.: Teams/Correo): _____

Canal para urgencias/incidentes: _____

Tiempos de respuesta esperados: _____

Qué se documenta y dónde (repositorio/drive/wiki): _____

4.2 Reuniones y coordinación

Reunión de seguimiento (frecuencia/duración): _____

Revisión con usuarios (frecuencia): _____

Revisión de riesgos y seguridad (frecuencia): _____

Regla: toda reunión debe cerrar con decisiones, responsables y fecha.

4.3 Gestión de tareas y visualización del trabajo

Herramienta de seguimiento (tablero/kanban): _____

Definición de prioridad (quién prioriza y cómo): _____

Bloqueos: cómo se reportan y escalan: _____

4.4 Control de cambios (alcance, requisitos, configuraciones)

Qué se considera cambio (alcance/req/config): _____

Quién aprueba cambios (Aprobador): _____

Ventana de cambios / despliegues: _____

Registro obligatorio (ticket/acta): _____

4.5 Calidad y ‘Definición de Hecho’ (DoD)

Criterios mínimos antes de marcar como “hecho”:

■ Pruebas realizadas ■ Evidencia registrada ■ Revisión por par ■ Documentación básica

Otros: _____

4.6 Seguridad, datos y privacidad (obligatorio en IA/ciberseguridad)

Principio de mínimo privilegio (accesos): _____

Manejo de credenciales (prohibido compartir por chat): _____

Tratamiento de datos (anonimización/consentimiento/uso permitido): _____

Bitácora de evidencias (auditoría/registros): _____

4.7 Normas de convivencia y conflicto

Regla de respeto y foco en evidencia (no personal): _____

Ruta de resolución de conflictos (quién media/escalamiento): _____

Feedback: usar modelo SBI (situación–comportamiento–impacto).

5. Plan de comunicación (Stakeholders)

Defina la comunicación por audiencias. En proyectos de IA/ciberseguridad, asegure mensajes claros sobre impactos, controles, límites y evidencias.

6. Checklist semanal del líder (recomendado)

- Tablero actualizado: tareas, prioridades y bloqueos visibles.
 - Decisiones registradas (acta/ticket) y comunicadas.
 - Riesgos revisados y responsables asignados (incluye datos y seguridad).
 - Avance validado con usuario/dueño del proceso cuando corresponda.
 - Cambios controlados: aprobaciones y evidencia.
 - Soporte a adopción: dudas respondidas y acciones de capacitación definidas.

7. Aprobación

Firma Patrocinador:	<input type="text"/>	Firma Líder del Proyecto:	<input type="text"/>
Nombre:	<input type="text"/>	Nombre:	<input type="text"/>
Cargo:	<input type="text"/>	Cargo:	<input type="text"/>
Fecha:	<input type="text"/>	Fecha:	<input type="text"/>